

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- v. -

KEONNE RODRIGUEZ and
WILLIAM LONERGAN HILL,

Defendants.

----- X

:

:

:

:

:

S3 24 Cr. 82 (RMB)

**THE GOVERNMENT’S OPPOSITION TO DEFENDANTS’
PRETRIAL MOTIONS**

NICOLAS ROOS
Acting Deputy United States Attorney,
Attorney for the United States,
Acting under Authority Conferred by
28 U.S.C. § 515

Andrew K. Chan
David R. Felton
Cecilia Vogel
Assistant United States Attorneys

- Of Counsel -

TABLE OF CONTENTS

PRELIMINARY STATEMENT	1
FACTUAL BACKGROUND.....	3
A. Background on Bitcoin.....	4
B. Background on Samourai Wallet	5
C. The Defendants’ Knowledge and Intent to Launder Criminal Proceeds.....	9
ARGUMENT.....	11
I. The Defendants’ Motion to Dismiss Should Be Denied.....	11
A. Applicable Law	11
B. Count Two Sufficiently Alleges a Conspiracy to Operate an Unlicensed Money Transmitting Business	13
C. Count One Sufficiently Alleges a Conspiracy to Commit Money Laundering	32
II. Hill’s Motion to Suppress and Request for a <i>Franks</i> Hearing Should Be Denied	43
A. The Search Warrant Affidavit for Hill’s Email Account Contained No False or Misleading Statements that Were Material to Probable Cause	43
B. The Search Warrant Affidavit for Hill’s Email Account Was Supported by Ample Probable Cause	50
C. Magistrate Judge Gorenstein’s Warrant Was Sufficiently Particularized and Not Impermissibly Overbroad.....	54
D. The Good Faith Exception Clearly Applies Here	61
E. The Full Extraction of Hill’s Email Account Is Needed for Purposes of Authenticating Identified Data at Trial	65
III. Hill’s Motion to Sever Should Be Denied	66
A. Applicable Law	67
B. Discussion	69
IV. The Defendants’ Demand for Additional Disclosure and a Hearing Should Be Denied.....	74
CONCLUSION.....	77

TABLE OF AUTHORITIES

Cases

<i>Allen v. Grist Mill Capital LLC</i> , 88 F.4th 383 (2d Cir. 2023)	66
<i>Bates v. United States</i> , 522 U.S. 23 (1997).....	28
<i>Boyce Motor Lines, Inc. v. United States</i> , 342 U.S. 337 (1952).....	11
<i>Costello v. United States</i> , 350 U.S. 359 (1956)	11
<i>Dalia v. United States</i> , 441 U.S. 238 (1979)	55
<i>Direct Sales Co. v. United States</i> , 319 U.S. 703 (1940)	40
<i>Florida v. Harris</i> , 568 U.S. 237 (2013)	51
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978).....	44, 45
<i>Givelify LLC v. Dep’t of Banking and Sec.</i> , 210 A.3d 393 (Pa. Commw. Ct. 2019).....	26
<i>Golino v. City of New Haven</i> , 950 F.2d 864 (2d Cir. 1991)	62
<i>Herring v. United States</i> , 555 U.S. 135 (2009).....	61
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983)	44
<i>Lomax v. Ortiz-Marquez</i> , 140 S. Ct. 1721 (2020)	28
<i>McBoyle v. United States</i> , 283 U.S. 25 (1931)	29
<i>Minnesota v. Murphy</i> , 465 U.S. 420 (1984)	70
<i>Moskal v. United States</i> , 498 U.S. 103 (1990).....	30
<i>Ponnapula v. Spitzer</i> , 297 F.3d 172 (2d Cir. 2002)	31
<i>Pulsifer v. United States</i> , 144 S.Ct. 718 (2024).....	30
<i>Ramsden v. United States</i> , 2 F.3d 322 (9th Cir. 1993).....	66
<i>Reiter v. Sonotone Corp.</i> , 442 U.S. 330 (1979)	18
<i>Richardson v. Marsh</i> , 481 U.S. 200 (1987)	67
<i>Rivera v. United States</i> , 928 F.2d 592 (2d Cir. 1991).....	44
<i>Russell v. United States</i> , 369 U.S. 749 (1962).....	12
<i>U.S. Postal Serv. v. C.E.C. Servs.</i> , 869 F.2d 184 (2d Cir. 1989)	57
<i>United States v. Aguilar</i> , 742 F. Supp. 3d 322 (E.D.N.Y. 2024).....	36
<i>United States v. Al Kassar</i> , 660 F.3d 128 (2d Cir. 2011)	38
<i>United States v. Alfonso</i> , 143 F.3d 772 (2d Cir. 1998)	12
<i>United States v. Aminov</i> , No. 23 Cr. 110 (MKV), 2024 WL 3104526 (S.D.N.Y. June 24, 2024).....	59
<i>United States v. Awadallah</i> , 349 F.3d 42 (2d Cir. 2003).....	44
<i>United States v. Babilonia</i> , 854 F.3d 163 (2d Cir. 2017).....	51
<i>United States v. Banki</i> , 685 F.3d 99 (2d Cir. 2012).....	14, 15, 23
<i>United States v. Bari</i> , 750 F.2d 1169 (2d Cir. 1984)	68, 69, 70, 71
<i>United States v. Barnes</i> , 979 F.3d 283 (5th Cir. 2020).....	67
<i>United States v. Barrett</i> , No. 23 Cr. 623 (JLR), 2025 WL 371084 (Feb. 3, S.D.N.Y. 2025)	56
<i>United States v. Beech-Nut Nutrition Corp.</i> , 871 F.2d 1181 (2d Cir. 1989).....	37
<i>United States v. Bondars</i> , 801 F. App’x 872 (4th Cir. 2020)	40
<i>United States v. Bongiovanni</i> , Nos. 19 Cr. 227 (JLS) (MJR), 23 Cr. 37 (JLS) (MJR), 2023 WL 3143894 (W.D.N.Y. Apr. 28, 2023)	72
<i>United States v. Bowen</i> , 689 F. Supp. 2d 675 (S.D.N.Y. 2010)	55

<i>United States v. Canfield</i> , 212 F.3d 713 (2d Cir. 2000).....	45
<i>United States v. Clark</i> , 638 F.3d 89 (2d Cir. 2011)	44
<i>United States v. Dawkins</i> , 999 F.3d 767 (2d Cir. 2021)	12, 33
<i>United States v. De La Pava</i> , 268 F.3d 157 (2d Cir. 2001)	2, 11
<i>United States v. DePalma</i> , 466 F. Supp. 920 (S.D.N.Y. 1979)	73
<i>United States v. E-Gold, Ltd.</i> , 550 F. Supp. 2d 82 (D.D.C. 2008).....	passim
<i>United States v. Elie</i> , No. 10 Cr. 336 (LAK), 2012 WL 383403 (S.D.N.Y. Feb. 7, 2012)	2
<i>United States v. Esters</i> , No. 21 Cr. 398 (EK), 2022 WL 16715891 (E.D.N.Y. Nov. 4, 2022).....	51
<i>United States v. Faiella</i> , 39 F. Supp. 3d 544 (S.D.N.Y. 2014).....	13, 23, 29
<i>United States v. Falcone</i> , 311 U.S. 205 (1940)	40
<i>United States v. Falso</i> , 544 F.3d 110 (2d Cir. 2008)	45
<i>United States v. Fares</i> , 95 F. App'x 379 (2d Cir. 2004).....	38
<i>United States v. Finkelstein</i> , 526 F.2d 517 (2d Cir. 1975).....	68
<i>United States v. Folks</i> , No. 20-3267-cr, 2021 WL 5987009 (2d Cir. Dec. 17, 2021)	56
<i>United States v. Fox</i> , No. 22 Cr. 53 (JLS) (JJM), 2023 WL 6940197 (W.D.N.Y. Oct. 20, 2023).....	71
<i>United States v. Freeman</i> , 688 F. Supp. 3d 1 (D.N.H. 2023)	19
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	56
<i>United States v. Gamez</i> , 1 F. Supp. 2d 176 (E.D.N.Y. 1998)	38
<i>United States v. Garcia</i> , 587 F.3d 509 (2d Cir. 2009).....	35
<i>United States v. Gatto</i> , 313 F. Supp. 3d 551 (S.D.N.Y. 2018)	58
<i>United States v. Gershman</i> , No. 16 Cr. 553 (BMC), 2018 WL 3038498 (E.D.N.Y. 2018).....	69, 70, 72
<i>United States v. Goklu</i> , No. 19 Cr. 386 (PKC), 2023 WL 184254 (E.D.N.Y. Jan. 13, 2023)	24, 25
<i>United States v. Goldberg</i> , 756 F.2d 949 (2d Cir. 1985).....	11
<i>United States v. Graziano</i> , 558 F. Supp. 2d 304 (E.D.N.Y. 2008).....	55
<i>United States v. Harmon</i> , 474 F. Supp. 3d 76 (D.D.C. 2020)	passim
<i>United States v. Jacobson</i> , 4 F. Supp. 3d 515 (E.D.N.Y. 2014)	63
<i>United States v. Jimenez Recio</i> , 537 U.S. 270 (2003).....	37
<i>United States v. Kidd</i> , 386 F. Supp. 3d 364 (S.D.N.Y. 2019)	57
<i>United States v. Kinzler</i> , 55 F.3d 70 (2d Cir. 1995).....	31
<i>United States v. Klump</i> , 536 F.3d 113 (2d Cir. 2008).....	44
<i>United States v. Lanier</i> , 520 U.S. 259 (1997).....	29, 30, 31
<i>United States v. Lauria</i> , 70 F.4th 106 (2d Cir. 2023)	44, 51
<i>United States v. Lebovits</i> , No. 11 Cr. 134 (SJ), 2012 WL 10181099 (E.D.N.Y. Nov. 30, 2012).....	55
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	61
<i>United States v. Levasseur</i> , 816 F.2d 37 (2d Cir. 1987)	46
<i>United States v. Levy</i> , No. 11 Cr. 62 (PAC), 2013 WL 787913 (S.D.N.Y. 2013).....	69, 72
<i>United States v. Maher</i> , 108 F.3d 1513 (2d Cir. 1997).....	36
<i>United States v. Mandell</i> , 710 F. Supp. 2d 368 (S.D.N.Y. 2010)	45
<i>United States v. Martin</i> , 411 F. Supp. 2d 370 (S.D.N.Y. 2006)	34

<i>United States v. Mazza-Alaluf</i> , 621 F.3d 205 (2d Cir. 2010).....	16, 17
<i>United States v. McDarragh</i> , 351 F. App'x 558 (2d Cir. 2009)	59
<i>United States v. McKenzie</i> , 13 F.4th 223 (2d Cir. 2021)	46, 50
<i>United States v. Messalas</i> , 612 F. Supp. 3d 93 (E.D.N.Y. 2020)	66
<i>United States v. Moore</i> , 968 F.2d 216 (2d Cir. 1992).....	62
<i>United States v. Motovich</i> , No. 21 Cr. 497 (WFK), 2024 WL 2943960 (E.D.N.Y. June 11, 2024)	59
<i>United States v. Murgio</i> , 209 F. Supp. 3d 698 (S.D.N.Y. 2016)	passim
<i>United States v. Nejad</i> , 436 F. Supp. 3d 707 (S.D.N.Y. 2020).....	50
<i>United States v. Neuman</i> , 621 F. App'x 363 (9th Cir. 2015).....	36
<i>United States v. Neumann</i> , No. 21 Cr. 439 (NSR), 2022 WL 3445820 (S.D.N.Y. Aug. 17, 2022)	25
<i>United States v. O'Connor</i> , 650 F.3d 839 (2d Cir. 2011).....	68
<i>United States v. Orozco-Prada</i> , 732 F.2d 1076 (2d Cir. 1984)	41
<i>United States v. Page</i> , 657 F.3d 126 (2d Cir. 2020)	67
<i>United States v. Paldiel</i> , No. 24 Cr. 329 (ARR), 2025 WL 524659 (E.D.N.Y. Feb. 18, 2025).....	37
<i>United States v. Percoco</i> , No. 16 Cr. 776 (VEC), 2017 WL 6314146 (S.D.N.Y. Dec. 11, 2017).....	34
<i>United States v. Purcell</i> , 967 F.3d 159 (2d Cir. 2020).....	56
<i>United States v. Rajaratnam</i> , 719 F.3d 139 (2d Cir. 2013)	44, 45, 46, 48
<i>United States v. Ray</i> , 541 F. Supp. 3d 355 (S.D.N.Y. 2021)	55, 58, 60, 64
<i>United States v. Raymonda</i> , 780 F.3d 105 (2d Cir. 2015)	61
<i>United States v. Riley</i> , 906 F.2d 841 (2d Cir.1990)	56, 60
<i>United States v. Rivera</i> , 750 F. Supp. 614 (S.D.N.Y. 1990).....	45
<i>United States v. Storm</i> , No. 23 Cr. 430 (KPF) (S.D.N.Y. October 3, 2024)	passim
<i>United States v. Rosa</i> , 626 F.3d 56 (2d Cir. 2010)	61
<i>United States v. Rosario</i> , No. 19 Cr. 807 (LAP), 2021 WL 5647879 (S.D.N.Y. Dec. 1, 2021).....	58
<i>United States v. Salameh</i> , 152 F.3d 88 (2d Cir. 1998).....	46
<i>United States v. Sampson</i> , 898 F.3d 270 (2d Cir. 2018).....	34
<i>United States v. Savin</i> , 349 F.3d 27 (2d Cir. 2003)	17
<i>United States v. Schlegel</i> , No. 06 Cr. 0550 (JS), 2009 WL 3837305 (E.D.N.Y. Nov. 16, 2009).....	69, 72
<i>United States v. Shareef</i> , 190 F.3d 71 (2d Cir. 1999)	67
<i>United States v. Shea</i> , No. 20 Cr. 412 (AT), 2023 WL 4551635 (S.D.N.Y. July 14, 2023)	37
<i>United States v. Silver</i> , 948 F.3d 538 (2d Cir. 2020).....	36
<i>United States v. Singh</i> , 390 F.3d 168 (2d Cir. 2004)	51
<i>United States v. Spinelli</i> , 352 F.3d 48 (2d Cir. 2003)	68
<i>United States v. Stavroulakis</i> , 952 F.2d 686 (2d Cir. 1992)	36, 37
<i>United States v. Sterlingov</i> , 573 F. Supp. 3d 28 (D.D.C. 2021)	23, 31, 42
<i>United States v. Stetkiw</i> , No. 18 Cr. 20579 (VAR), 2019 WL 417404 (E.D. Mich. Feb. 1, 2019).....	25

<i>United States v. Stokes</i> , 733 F.3d 438 (2d Cir. 2013)	61
<i>United States v. Stringer</i> , 730 F.3d 120 (2d Cir. 2013)	11, 12
<i>United States v. Superior Growers Supply, Inc.</i> , 982 F.2d 173 (6th Cir. 1993)	40
<i>United States v. Svoboda</i> , 347 F.3d 471 (2d Cir. 2003)	37
<i>United States v. Triumph Capital Group</i> , 260 F. Supp. 2d 432 (D. Conn. 2002)	69
<i>United States v. Ulbricht</i> , 31 F. Supp. 3d 540 (S.D.N.Y. 2014)	passim
<i>United States v. Velastegui</i> , 199 F.3d 590 (2d Cir. 1999)	25
<i>United States v. Vilar</i> , 729 F.3d 62 (2d Cir. 2013)	12
<i>United States v. Vilar</i> , No. 05 Cr. 621 (KMK), 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007)	45
<i>United States v. Wallace</i> , 85 F.3d 1063 (2d Cir. 1996)	38
<i>United States v. Wallace</i> , No. 24 Cr. 411 (MKV), 2025 WL 1435066 (S.D.N.Y. May 19, 2025)	56
<i>United States v. Wedd</i> , 993 F.3d 104 (2d Cir. 2021)	33
<i>United States v. Weiner</i> , 152 F. App'x 38 (2d Cir. 2005)	38
<i>United States v. Welch</i> , No. 24 Cr. 79 (ALC), 2025 WL 1380063 (S.D.N.Y. May 13, 2025)	51
<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017)	57, 63
<i>United States v. Wilburn</i> , Nos. 19 Cr. 108 (EK) (VMS), 19 Cr. 139 (EK) (VMS), 2024 WL 1142297 (E.D.N.Y. Mar. 15, 2024)	66
<i>United States v. Williams</i> , 504 U.S. 36 (1992)	12
<i>United States v. Wilson</i> , 11 F.3d 346 (2d Cir. 1993)	68, 69, 72
<i>United States v. Wittig</i> , 575 F.3d 1085 (10th Cir. 2009)	37
<i>United States v. Yannotti</i> , 541 F.3d 112 (2d Cir. 2008)	12
<i>United States v. Zambrano</i> , 776 F.2d 1091 (2d Cir. 1985)	41
<i>Zafiro v. United States</i> , 506 U.S. 534 (1993)	67

Statutes

18 U.S.C. § 1956	passim
18 U.S.C. § 1960	passim
31 U.S.C. § 5312	33
31 U.S.C. § 5330	passim

PRELIMINARY STATEMENT

The Government submits this memorandum in opposition to pretrial motions by Defendants Keonne Rodriguez and William Lonergan Hill, (Dkts. 98, 99, 103, and 107), which include: (1) a motion to dismiss the indictment joined by both defendants (Dkt. 107); (2) a motion to suppress evidence found during a court-authorized search of Hill's personal email account (Dkt. 99); (3) a motion for severance by Hill (Dkt. 103); and (4) a motion joined by both defendants to compel additional disclosures and for a hearing regarding the Government's disclosure of a call with FinCEN on August 23, 2023 (Dkt. 98).¹ The defendants' motions should be denied in their entirety.

The Indictment in this case alleges that for nearly a decade, the Samourai Wallet cryptocurrency mixing service ("Samourai") operated as a haven for criminals to engage in large-scale money laundering. Samourai laundered at least \$250 million in criminal proceeds for a host of cyber criminals, including the Silk Road darknet market, the Hydra darknet market, as well as millions of dollars from a series of computer hacks and other cyber intrusions. As alleged in the Indictment, the defendants developed, marketed, paid for, and operated Samourai, and they personally reaped millions of dollars in profits from it. The defendants operated Samourai knowing and intending that Samourai would be used to launder and conceal criminal proceeds, thereby frustrating the efforts of victims and law enforcement to trace and recover the illicit funds. On numerous occasions, the defendants actively encouraged criminals to use Samourai as a tool to engage in money laundering.

¹ Rodriguez also moved to suppress evidence recovered from a safe during a search of his home. (Dkt. 101). For the reasons stated in the Government's letter dated June 24, 2025, Rodriguez has agreed to withdraw the motion. (Dkt. 110).

The Government responds to each of the defendants' arguments in detail below, but two general points are worth noting at the outset to provide relevant context to assessing the defendants' motion to dismiss:

First, as this Court is well aware, dismissal of an Indictment is an “‘extraordinary remedy’ reserved only for extremely limited circumstances implicating fundamental rights.” *United States v. De La Pava*, 268 F.3d 157, 165 (2d Cir. 2001) (citation omitted). The defendants cannot meet their heavy burden here where the detailed, 29-page, 50-paragraph speaking Indictment sets forth the criminal conduct underlying the two counts of the Indictment in far more detail than necessary. The defendants cannot obtain dismissal of the Indictment simply by making factual assertions about their own contested view as to how Samourai operated and executed cryptocurrency transactions on behalf of their customers. Similarly, the defendants cannot obtain dismissal of the Indictment based on their own self-serving assertions of their intent or lack thereof when they created and operated Samourai. Simply put, “there is no summary judgment in criminal cases.” *United States v. Elie*, No. 10 Cr. 336 (LAK), 2012 WL 383403, at *1 (S.D.N.Y. Feb. 7, 2012). Ultimately, it is for the jury to decide whether the defendants participated in a conspiracy with each other and their customers to engage in money laundering and in knowingly transmitting criminal proceeds.

Second, the Indictment alleges, and the Government expects to prove at trial, that the defendants knew and intended that criminal proceeds would be laundered using Samourai, and they encouraged and openly invited their users to engage in money laundering by sending their criminal proceeds to Samourai. (See Dkt. 109 (“Indictment” or “Ind.”) ¶¶ 1, 19-35).² This is not

² On June 24, 2025, the grand jury returned the S3 superseding indictment in this case. The

a case in which the operators of a cryptocurrency mixer might be held criminally liable when they learn that a small subset of their customers may be misusing their service to engage in money laundering. Rather, the Government's evidence at trial will show that the defendants designed Samourai to be used as a tool for money laundering, and they specifically intended and repeatedly solicited customers to use Samourai to launder the proceeds of criminal activity.

As discussed below, the defendants' other pretrial motions are similarly lacking in merit.

FACTUAL BACKGROUND

As alleged in the Indictment, this case arises from the defendants' creation and operation of Samourai Wallet, a cryptocurrency mixing service that executed anonymous, virtually untraceable cryptocurrency transfers for its customers. The defendants implemented multiple features in Samourai that together allowed it to conceal the connection between deposits and withdrawals, making these transfers untraceable on the publicly available blockchain. These features were of immense value to cybercriminals and other criminals, who used the defendants' service to launder the proceeds of various criminal exploits. The defendants intentionally solicited cybercriminals as their customers. The defendants were also fully aware of the criminal funds flowing through Samourai, and yet continued to operate Samourai, execute transactions

superseding indictment does not add new charges. It includes the following substantive updates compared to the S2 superseding indictment: (1) extending the time period of the conspiracies charged in Count One and Two until the time of the defendants' arrests in April 2024; (2) in Count One, changing the definition of "financial transaction" to "movement of funds by wire or other means" instead of "involving the use of a financial institution"; (3) in Count One, adding the statutory citation to 21 U.S.C §§ 841 and 846 as specified unlawful activity, based on allegations already included in the speaking portion of the S2 superseding indictment; (4) in Count Two, eliminating the (b)(1)(B) object of the conspiracy to violate 18 U.S.C. § 1960; and (5) adding descriptions of additional evidence, all of which has previously been produced to the defendants in discovery.

involving criminal proceeds, encourage criminals to use Samourai to engage in money laundering, and reap profits from this conduct.

The Indictment provides an overview of some of the facts the Government expects to prove at trial. This factual background section summarizes some of these facts and highlights some areas of disagreement with the defendants' characterization of the facts, but neither this background section nor the Indictment is intended as a complete proffer of the Government's anticipated proof at trial. Of course, on a motion to dismiss, the allegations in the Indictment must be accepted as true, and the defendants' own contested version of events does not control.

A. Background on Bitcoin

Bitcoin ("BTC") is a decentralized form of electronic currency, or cryptocurrency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer to peer" network. (Ind. ¶¶ 4-5). BTC is stored as a balance in a bitcoin "address," designated by a string of letters and numbers. The owner of the BTC can manage the bitcoin address with software or hardware known as a "wallet," which is controlled by a "private key" known to the wallet's owner. A private key is akin to a PIN or password that allows a user the ability to access and transfer value associated with the bitcoin address. Once a bitcoin user funds an address in his or her wallet with BTC, the user can then use the BTC to conduct financial transactions, by transferring BTC to the bitcoin address of another user. This is accomplished over the Internet, by sending a message announcing the transfer to the bitcoin peer-to-peer network. (Ind. ¶¶ 6-7).

All BTC transactions are recorded on a public online ledger known as the "blockchain," which is stored on bitcoin's peer-to-peer network. The bitcoin blockchain records the balance

held in each bitcoin address and records all BTC transactions between addresses. This public ledger serves to prevent any user from spending more BTC than the user holds in his or her bitcoin address. The public nature of the blockchain means that the movement of funds over the bitcoin blockchain can be traced. (Ind. ¶¶ 7-8).

B. Background on Samurai Wallet

Defendants Rodriguez and Hill began developing Samurai in or around 2015. Samurai was a mobile cellphone application that users could download onto their cellphones, and the Samurai application was downloaded over 100,000 times. After users downloaded Samurai, they could store their private keys for any BTC addresses they controlled inside of the Samurai program. The private keys remained stored on a user's cellphone, but Samurai operated a centralized server (the "Coordinator Server"), managed by the defendants, that, among other things, supervised, executed, and facilitated transactions between Samurai users, and to do so, created new BTC addresses to which Samurai sent users' BTC. (Ind. ¶ 9).

The defendants designed Samurai to offer at least two features intended to assist individuals engaged in criminal conduct to conceal the source of the proceeds of their criminal activities: First, Samurai offered a cryptocurrency mixing service known as "Whirlpool," which coordinated batches of cryptocurrency exchanges between groups of Samurai users to prevent tracing of criminal proceeds by law enforcement on the blockchain. Second, Samurai offered a service called "Ricochet," which allowed a Samurai user to build in additional and unnecessary intermediate transactions (known as "hops") when sending cryptocurrency from one address to another address.

1. Whirlpool Transactions

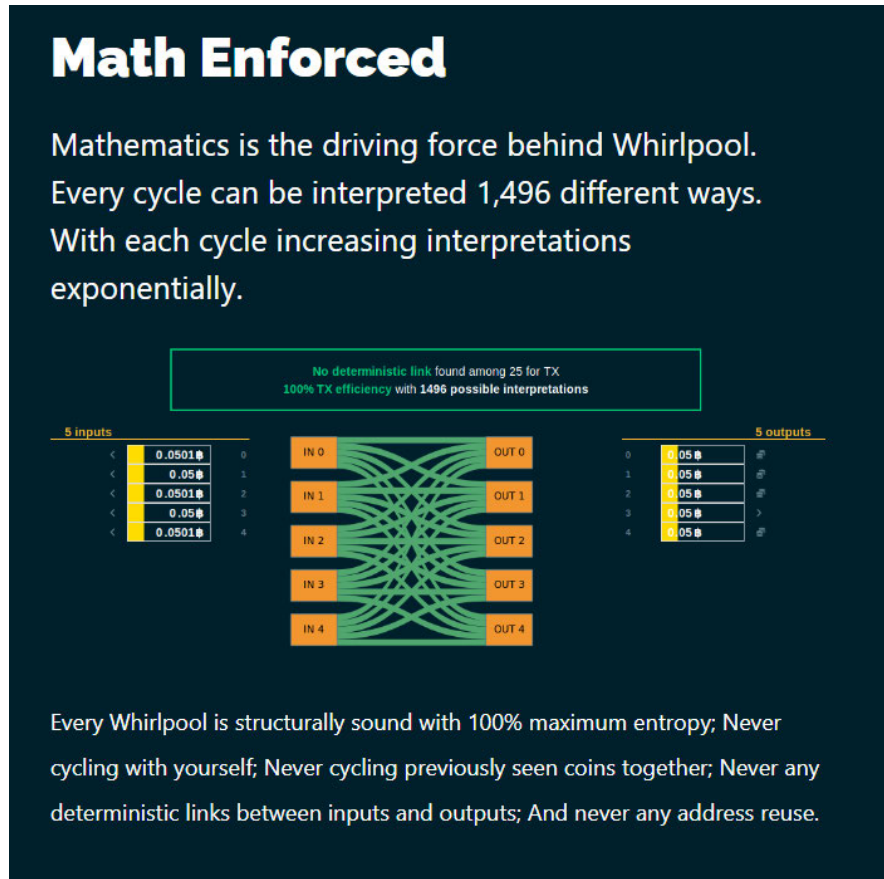
To use the "Whirlpool" feature, which the defendants introduced in or around April 2019,

a Samurai user selected an amount of BTC that they wished to mix and a particular Samurai pool in which they wished to mix that BTC. Each pool was designed to accept BTC in a set increment and had a flat fee to contribute BTC to the pool. The pools were designed for denominations of 0.001 BTC, 0.01 BTC, 0.05 BTC, and 0.5 BTC. (Ind. ¶ 15). The Whirlpool feature functioned as follows:

First, once a user contributed cryptocurrency from their Samurai wallet to be sent into the Whirlpool, the cryptocurrency was “cut down” into the correct sizes for a chosen pool. Samurai also collected its fee and the mining fees from the transaction. Then the user’s funds waited to join a mix. For example, if a user wished to contribute 1 BTC into the 0.05 BTC pool, the Samurai software on the user’s cellphone broadcasted a transaction on the blockchain transferring the 1 BTC into 19 addresses, each containing approximately 0.05 BTC, in addition to the mining fees necessary for broadcasting the subsequent transactions to the blockchain. Each of the 19 addresses containing approximately 0.05 BTC served as an “input” in a Whirlpool transaction. The broadcasted transaction also sent Samurai’s fees from the user to an address designated by the Samurai software. (Ind. ¶ 16(a)).

Second, through the Coordinator Server that the defendants operated, the Samurai application on a user’s cellphone communicated with other Samurai users, and the Samurai Coordinator Server randomly selected four other inputs already in the selected pool to be mixed with the new incoming input and communicated that information to each user. The Samurai application on each user’s cellphone then broadcasted the transaction to the blockchain in which all five inputs (each a separate address) were then transferred to five outputs (each a separate address). The defendants designed Samurai to automatically generate these addresses that were used as inputs and outputs on behalf of Samurai’s users, although the private keys for the

addresses were stored in each user's individual cellphone and not shared with Samourai's employees. The Indictment contains a graphical representation posted on Samourai's website of the five input and five output transaction:



In the example described above, each new unit of 0.05 BTC contributed by the user into the 0.05 BTC pool will combine with four other units of 0.05 BTC already in the pool from up to four other users to engage in a five-input-five-output transaction. (Ind. ¶ 16(b)).

Finally, after the mix is complete, Samourai continued to automatically mix the outputs with other batches of cryptocurrency that were in the same pool indefinitely as new cryptocurrency entered the pool, until a user chose to remove their cryptocurrency from the Whirlpool. In other words, each time a transaction in the Whirlpool occurred, one new input and four old inputs already in a pool engaged in a five-input-five-output transaction. All these transactions were coordinated

by Samurai's Coordinator Server. The defendants incentivized users to keep their cryptocurrency in the Whirlpool (and therefore generate additional liquidity in the pool) by programming Samurai to offer subsequent remixes free of charge. Mining fees for the broadcasting of these subsequent cryptocurrency transactions were covered by new BTC inputs entering the pool. Samurai's Whirlpool feature generated over \$3 million in fees for the defendants—the large majority of which the defendants also stored and laundered in the Whirlpool as a source of additional liquidity. (Ind. ¶ 16(c)).

2. Ricochet Transactions

The defendants designed Samurai to include a feature known as “Ricochet” that further assisted customers in obfuscating the link between their deposits and withdrawals. The “Ricochet” feature built in additional and unnecessary intermediate transactions (known as “hops”) when sending cryptocurrency from one address to another address to further obscure the source and ownership of funds. (Ind. ¶ 17). To use the Ricochet feature, which was introduced by the defendants in or around 2017, a Samurai user selected the amount of BTC that they wished to send and the destination address where the BTC was to be sent. The user could also decide whether they wanted the Ricochet transaction to occur instantly or over a designated amount of time. Samurai's Coordinator Server, controlled by the defendants, provided an address where their fees were received prior to the execution of the series of Ricochet transactions. The Samurai application then created the series of BTC transactions for each Ricochet, including the creation of new addresses, where were transmitted to Samurai's Coordinator Server. As with the Whirlpool feature, Samurai automatically generated the new cryptocurrency addresses that were used for these transactions, although the private keys for these addresses were stored in each user's individual cellphone and not shared with Samurai's employees. Samurai's Ricochet

feature generated over \$1 million in fees for the defendants, the large majority of which they also laundered through Samurai's Whirlpool feature. (Ind. ¶ 18).

C. The Defendants' Knowledge and Intent to Launder Criminal Proceeds

As the Indictment alleges, the defendants specifically intended and encouraged their customers to launder criminal proceeds through Samurai. (Ind. ¶¶ 1, 19-35). For example, when asked by an associate what "mixing" was, Rodriguez explained that it was "money laundering for bitcoin." (Ind. ¶ 20). As another example, on Dread, a dark web message board featuring discussions about darknet marketplaces, Hill expressly advertised Samurai as a money laundering service. In the subforum titled "Laundromat," bearing the banner photograph of a masked criminal washing money in a bathtub (*i.e.*, laundering or cleaning his dirty money), and in a post titled "How to clean dirty BTC," a Dread user asked what were the most "[s]ecure methods to clean dirty BTC" so that the BTC would become "untraceable, clean" and the Dread user would "never get caught." Hill responded by criticizing a competitor mixer ("Mixer-1") by directing the Dread user to "Avoid [Mixer-1] at all costs" and, instead, encouraged the Dread user to use Samurai, writing that "Samurai Whirlpool is a much better option" to clean dirty BTC. (Ind. ¶ 21). Rodriguez was aware of Hill's activities on Dread, noting that "we're making a space on the dark net boards, dread in particular" and Hill "has been doin[g] a lot of work there." (Ind. ¶ 23). Moreover, Rodriguez announced in September 2019 that Iran was the second largest country of Samurai downloads after the United States, and he followed up with a message in December 2020 actively encouraging users from Iran to "run their BTC acquired via Iranian exchanges in Whirlpool"—a plain reference to the fact that Iranian exchanges are sanctioned entities under the International Emergency Economic Powers Act ("IEEPA"). (Ind. ¶ 28). Further, Samurai's Twitter account, which was operated by Rodriguez, posted a message in or around June 2022,

encouraging Russian oligarchs seeking to circumvent sanctions to use Samourai. (Ind. ¶ 27). The defendants' marketing materials also discussed how Samourai's customer base was intended to include criminals, including references to "Restricted Markets," "Dark/Grey Market Participants," and "Illicit Activity." (Ind. ¶¶ 32-34).

Similarly, in or around July 2020, Rodriguez actively solicited and encouraged criminals to use Samourai to launder crime proceeds of a hack of a social media company ("Social Media Company-1"). Here, after a third party encouraged the hackers to "use @SamouraiWallet whirlpool to mix out once you are done collecting or decide to take profits" in order to "protect you from being found," Rodriguez used Samourai's Twitter account to personally encourage the hackers to "[f]eed" and "[s]end" the hack crime proceeds into Samourai's Whirlpool, including posting a 20% discount code so that the hackers could get a discount on the sizable fees that Samourai collects from all Whirlpool transactions. (Ind. ¶ 25).

Beyond these public messages, in private messages the next day, an associate complained to Rodriguez about the hackers using Mixer-1 instead of Samourai, musing: "why oh why can't someone high profile use Whirlpool?!" (Ind. ¶ 25). Rodriguez responded: "We were aware of them entering [Mixer-1] 6 hours ago . . . trust me, we're all disappointed." (Ind. ¶ 25). Rodriguez's disappointment at the hackers' decision not to use Samourai leaves no doubt regarding the defendants' desire and intent for the proceeds of "high profile" criminal activities to be laundered using Samourai. (Ind. ¶ 25). Likewise, in response to a public statement by Mixer-1 expressing remorse that the Social Media Company-1 hackers used Mixer-1 to launder crime proceeds, Hill criticized Mixer-1 both for its apology and for its inadequate concealment of the crime proceeds, which he predicted would lead to "inevitable arrests." (Ind. ¶ 25).

At trial, the Government will present additional examples of the defendants actively soliciting and encouraging criminals to use Samourai to launder their criminal proceeds.

ARGUMENT

I. The Defendants’ Motion to Dismiss Should Be Denied

The defendants move to dismiss the two charges in the Indictment on the basis that the Indictment’s allegations are insufficient and legally defective. (Dkt. 107). That motion is meritless. As discussed below, the charges track the relevant statutes, and the defendants’ alleged misconduct falls within the heartland of what these statutes prohibit. There can be no serious dispute that the 29-page Indictment returned by the grand jury in this case alleges every element of each charged offense and fairly informs the defendants of the charges against which they must defend. The Indictment is sufficient on this ground alone. *See United States v. Stringer*, 730 F.3d 120, 124 (2d Cir. 2013).

A. Applicable Law

On a pretrial motion to dismiss pursuant to Fed. R. Crim. P. 12(b), the allegations of the indictment must be taken as true. *See Boyce Motor Lines, Inc. v. United States*, 342 U.S. 337, 343 n.16 (1952); *United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985).³ The law is well settled that “[a]n indictment returned by a legally constituted and unbiased grand jury . . . if valid on its face, is enough to call for trial of the charge on the merits.” *Costello v. United States*, 350 U.S. 359, 363 (1956). The dismissal of an indictment is an “‘extraordinary remedy’ reserved only for extremely limited circumstances implicating fundamental rights.” *De La Pava*, 268 F.3d at 165 (2d Cir. 2001).

³ Unless otherwise noted, case quotations omit internal quotation marks, citations, and previous alterations.

“Pursuant to Federal Rule of Criminal Procedure 7, ‘the indictment or information must be a plain, concise, and definite written statement of the essential facts constituting the offense charged.’” *United States v. Vilar*, 729 F.3d 62, 80 (2d Cir. 2013). To satisfy this rule, “an indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime.” *United States v. Yannotti*, 541 F.3d 112, 127 (2d Cir. 2008). Only in “very rare cases,” such as those where the indictment alleges refusal to answer questions before Congress, must an indictment specify “how a particular element of a criminal charge will be met.” *Stringer*, 730 F.3d at 125-26 (discussing the special case of *Russell v. United States*, 369 U.S. 749 (1962)). Otherwise, “[a]n indictment is sufficient if it first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense.” *Stringer*, 730 F.3d at 124; *see also Yannotti*, 541 F.3d at 127.

Where a defendant has been given sufficient notice of the charges against him by means of, for example, a criminal complaint or discovery, prejudice will not have been shown, and the indictment should stand. *See, e.g., Stringer*, 730 F.3d at 124-25; *Yannotti*, 541 F.3d at 127. Moreover, it is well settled that, “[u]nless the government has made what can fairly be described as a full proffer of the evidence it intends to present at trial,” a facially valid indictment is not subject to challenge based on the quality or quantity of evidence. *United States v. Alfonso*, 143 F.3d 772, 776 (2d Cir. 1998); *see United States v. Williams*, 504 U.S. 36, 54 (1992). To that end, “at the indictment stage, [courts] do not evaluate the adequacy of the facts to satisfy the elements of the charged offense.” *United States v. Dawkins*, 999 F.3d 767, 780 (2d Cir. 2021). Rather, “[t]hat is something [courts] do after trial.” *Id.* This is consistent with the well-established principle that summary judgment proceedings “do[] not exist in federal criminal procedure.” *Id.*

B. Count Two Sufficiently Alleges a Conspiracy to Operate an Unlicensed Money Transmitting Business

1. Applicable Law

Count Two alleges that the defendants conspired with others to “conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business,” in violation of Title 18, United States Code, Section 1960. (Ind. ¶ 47). Section 1960 defines “money transmitting” to include “transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier.” 18 U.S.C. § 1960(b)(2); *see United States v. Murgio*, 209 F. Supp. 3d 698, 706 (S.D.N.Y. 2016). Courts have uniformly held, and the defendants do not dispute in their motion, that “funds” and “money” for purposes of this statute include cryptocurrencies. *E.g.*, *Murgio*, 209 F. Supp. 3d at 705-10 (Bitcoin exchange covered by 18 U.S.C. § 1960); *United States v. Faiella*, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014) (“Bitcoin clearly qualifies as ‘money’ or ‘funds’” for purposes of 1960 prosecution); *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. 2020) (applying Section 1960 to bitcoin mixing service).

Section 1960 lists three independent ways in which a money transmitting business can be “unlicensed,” in violation of the statute.

[T]he term “unlicensed money transmitting business” means a money transmitting business which affects interstate or foreign commerce in any manner or degree and—

- (A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;
- (B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;

18 U.S.C. § 1960(b)(1)(A)-(C). In this case, section 1960(b)(1)(C) is the sole alleged object of the conspiracy charged in Count Two of the Indictment.⁴

The Indictment alleges that the defendants conducted, controlled, managed, supervised, directed, and owned all and part of Samourai, a money transmitting business which involved the transportation and transmission of funds known to the defendants to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, in violation of 18 U.S.C. § 1960(b)(1)(C). Ind. ¶ 47). For purposes of Section 1960(b)(1)(C), the Government must prove that the business engaged in “money transmitting” as that term is defined in Section 1960(b)(2), and that the defendants knew that the business transferred or transmitted funds that were derived from a criminal offense or that were intended to be used to promote or support unlawful activity.

Finally, the use of the word “business” in Section 1960 means that the Government must prove that the defendants did more than engage in a “single, isolated transmission of money.” *United States v. Banki*, 685 F.3d 99, 114 (2d Cir. 2012), *as amended* (Feb. 22, 2012). Rather, “under § 1960 a ‘business’ is an enterprise that is carried on for profit or financial gain.” *Id.*; *see*

⁴ The S2 superseding indictment alleged that the objects of the conspiracy charged in Count Two included both Sections 1960(b)(1)(B) and (b)(1)(C). On May 15, 2025, the Government informed the defendants that, in response to a memorandum dated April 7, 2025, “Ending Regulation by Prosecution,” by the Deputy Attorney General, it did not intend to proceed to trial on Section 1960(b)(1)(B), that is, the first object of Count Two of the S2 superseding Indictment. On June 24, 2025, the grand jury returned the S3 superseding indictment, which, among other things, eliminated the Section 1960(b)(1)(B) object of Count Two.

also id. at 113 (holding that district court erred in not instructing jury that a “money transmitting business” is “(1) an enterprise (not a single transaction) (2) that is conducted for a fee or profit”).

2. Title 31, United States Code, Section 5330 and FinCEN Regulations and Guidance Are Irrelevant to the Charged Object of Title 18, United States Code, Section 1960(b)(1)(C)

The defendants’ motion to dismiss Count Two on the basis that Samourai is not an unlicensed money transmitting business relies heavily on the definitions in Title 31, United States Code, Section 5330, FinCEN regulations, and FinCEN guidance. (Dkt. 107 at 2-4, 12-14). Section 5330 and FinCEN regulations and guidance, however, are irrelevant to violations of 18 U.S.C. § 1960(b)(1)(C)—the only provision of Section 1960 with which the defendants are now charged. The Court should not look to Section 5330 or to FinCEN regulations or guidance to determine whether Samourai was a money transmitting business in violation of Section 1960(b)(1)(C)—a statute that FinCEN is not charged with administering or enforcing.

As described above, Section 1960 provides for three independent ways a money transmitting business can be unlicensed: (1) operating without a state money transmitting license; (2) failing to comply with the registration requirements of Title 31, United States Code, Section 5330; or (3) knowingly otherwise transmitting funds originating from or promoting criminal activity. 18 U.S.C. §§ 1960(b)(1)(A)-(C); *see United States v. E-Gold, Ltd.*, No. 07-CR-109-ABJ-ZMF, 2022 WL 521612, at *7 (D.D.C. Feb. 16, 2022) (noting defendants pled guilty to each of Section 1960’s “three independent” violations). Only Section 1960(b)(1)(B), which criminalizes a money transmitting business’s failure to register as required by federal law, incorporates the registration requirements of 31 U.S.C. § 5330. Section 5330 is a provision of the Bank Secrecy Act. It governs federal registration of money transmitting businesses and includes separate statutory definitions for “money transmitting business” and “money transmitting service”

“for the purposes of this section”, *i.e.*, for the purpose of the Bank Secrecy Act. 31 U.S.C. §5330(d). The definitions of “money transmitting” and “money transmitting business” in Section 1960 and Section 5330, respectively, are not coextensive. Transcript of September 25, 2024 Conference (“Tr.”) at 2, *United States v. Roman Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y. October 3, 2024), ECF No. 84 (“to the extent that anyone . . . is arguing that the definitions of ‘money transmitting’ in Sections 1960 and 5330 are co-extensive. I do not believe that to be the case.”).

As stated above, Section 1960 defines “money transmitting” as:

includ[ing] transferring of funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier[.]

18 U.S.C. § 1960(b)(2). Section 5330, on the other hand, defines “money transmitting business” to mean:

any business other than the United States Postal Service which—

(A) provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers’ checks, and other similar instruments or any other person who engages as a business in the transmission of currency, funds, or value that substitutes for currency, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system[.]

31 U.S.C. § 5330(d)(1). Because Section 1960 has its own definition of “money transmitting” in Section 1960(b)(2), “Section 1960 does not borrow the definition of ‘money transmitting business’ from Section 5330.” *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 89 (D.D.C. 2008); *see also United States v. Mazza-Alaluf*, 621 F.3d 205, 210 (2d Cir. 2010) (rejecting defendant’s attempt to “import[] the § 5330(d)(1)(B) definition of ‘money transmitting business’ into § 1960”).

For several reasons, the definition of “money transmitting business” in 31 U.S.C. § 5330 does not apply to 18 U.S.C. § 1960. First, “the construction of the statute alone” shows that the definitions in Section 5330 do not apply to Section 1960. *E-Gold, Ltd.*, 550 F. Supp. 2d at 90. Rather, Section 1960(b)(2) contains its own definition of “money transmitting,” which follows the three independent ways outlined in Sections 1960(b)(1)(A)–(C) in which a money transmitting business can be unlicensed (and hence criminally unlawful), indicating it applies to each of the subsections. *See id.* Second, importing Section 5330’s definition of “money transmitting business” into Section 1960 “would render superfluous” Section 1960’s own definition of “money transmitting” and would run “afoul of well-settled canons of statutory interpretation.” *Mazza-Alaluf*, 621 F.3d at 210; *E-Gold, Ltd.*, 550 F. Supp. 2d at 92-93. Third, Section 5330(d) states that its definitions apply only “[f]or purposes of this section,” thus explicitly limiting the application of the Section 5330(d) definitions to other statutes. *Mazza-Alaluf*, 621 F.3d at 210 (citing *United States v. Savin*, 349 F.3d 27, 36-37 (2d Cir. 2003)); *E-Gold, Ltd.*, 550 F. Supp. 2d at 92 (refusing to incorporate Section 5330(d)’s definitions into Section 1960 because “it is a widely accepted principle of statutory interpretation that if a word is defined to mean something particular ‘in this section,’ then it will be given that definition only in that section and will be given either its ordinary meaning in the rest of the statute, or if it is defined in [another] definition section, the meaning given there”). Indeed, “there is a strong presumption that Congress did not intend for the definition in Section 5330 to apply to Section 1960” because “[i]f Congress had wanted to define the phrase ‘money transmitting business’ to have the exact same meaning in Section 1960 as it has in Section 5330, it plainly could have done so considering that it amended Section 1960 to include a reference to Section 5330 at the same time that it enacted Section 5330.” *Id.* at 91-92 (citing Pub. L. No. 103–325, § 408(c), 108 Stat. 2160, 2249–52). But Congress chose not to.

Accordingly, this Court should rely solely on the definition of “money transmitting” in Section 1960(b)(2).

Moreover, in this case the Court need not even decide the relationship between the definition of “money transmitting business” in Section 5330(d) and Section 1960 generally because the defendants are charged only with violating Section 1960(b)(1)(C), which clearly does not reference or incorporate Section 5330 in any way. “[T]he use of the conjunctive ‘or’ makes it apparent that subsection (b)(1)(B), including the reference to Section 5330, does not apply laterally to subsections (b)(1)(A) or (b)(1)(C).”⁵ *Id.* at 90 (citing *Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979) (reiterating that “[c]anons of construction ordinarily suggest that terms connected by a disjunctive be given separate meanings, unless the context dictates otherwise”). Indeed, neither licensing nor registration are elements of Section 1960(b)(1)(C), and thus there is no basis to incorporate into Section 1960(b)(1)(C) components of Section 5330, which governs federal registration and licensing of money transmitting businesses.

Finally, the FinCEN administrative ruling and guidance regarding virtual currencies cited by the defendants is not relevant to the definition of “money transmitting” in Section 1960(b)(2) for the purpose of determining whether a money transmitting business has violated Section 1960(b)(1)(C). Neither the FinCEN administrative ruling nor the FinCEN guidance cited by the defendants mention Section 1960; instead, they state that they provide guidance regarding virtual currencies under the Bank Secrecy Act, which is unrelated to Section 1960(b)(1)(C). *See*

⁵ It is as nonsensical to incorporate the definition of “money transmitting business” from Section 5330(d) to Section 1960(b)(1)(C) as it would be to incorporate that definition to Section 1960(b)(1)(A). Section 1960(b)(1)(A) criminalizes operating a money transmitting business without a *state* license, and thus, like Section 1960(b)(1)(C), in no way implicates 31 U.S.C. § 5330, which sets forth the requirements for *federal* registration of a money transmitting business.

FinCEN, *Application of FinCEN Regulations to Virtual Currency Mining Operations* (Jan. 30, 2014) (responding to a company’s request for an administrative ruling “about [the Company]’s possible status as a money services business . . . *under the Bank Secrecy Act*) (emphasis added); FinCEN Guidance, FIN-2019-G001, *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Currencies* (May 9, 2019) (“issuing this interpretive guidance to remind persons *subject to the Bank Secrecy Act* . . . how FinCEN regulations relating to money services businesses . . . apply to certain business models”) (emphasis added). The FinCEN administrative ruling and guidance are therefore immaterial to the conduct charged here. *See United States v. Freeman*, 688 F. Supp. 3d 1, 14 (D.N.H. 2023) (rejecting argument that FinCEN guidance was relevant to Section 1960 charge because the “indictment neither depends on nor references the FinCEN guidance,” and because the FinCEN guidance did not mention Section 1960 but instead provided guidance “under the Bank Secrecy Act”), *appeal dismissed*, No. 23-1771, 2024 WL 1191154 (1st Cir. Jan. 22, 2024); *Murgio*, 209 F. Supp. 3d at 709 (rejecting argument that FinCEN guidance regarding virtual currencies was relevant to interpreting “funds” in Section 1960 where the “FinCEN guidance does not even mention § 1960, much less purport to interpret the statute’s use of the word ‘funds’”).

3. Count Two Sufficiently Alleges that the Defendants Engaged in Unlicensed Money Transmitting in Violation of 18 U.S.C. § 1960(b)(1)(C)

The defendants’ motion argues that the Indictment does not allege the existence of a money transmitting business because it purportedly does not allege that Samourai or the defendants “transferred Bitcoin on behalf of someone to someone else.” (Dkt. 107 at 11). Instead, the defendants argue, the Indictment alleges “users—not Samourai or its providers—transmitted their own cryptocurrency and simply used the app to maintain the privacy of their financial transactions”

because Samourai did not have custody of users' private keys for their bitcoin.⁶ (Dkt. 107 at 11). This argument fails. The Indictment sufficiently tracks the statutory language and is therefore sufficient to survive a motion to dismiss. However, the facts alleged in the speaking portions of the Indictment are also plainly sufficient to allege a violation of Section 1960(b)(2). Specifically, the Indictment alleges that the defendants, through Samourai, were engaged in money transmitting, as defined in Section 1960(b)(2), and the fact that Samourai users kept custody of the private keys for their bitcoin does not negate the sufficiency of the allegation.

“Money transmitting includes transferring funds on behalf of the public *by any and all means* including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier.” 18 U.S.C. § 1960(b)(2) (emphasis added). The Indictment satisfies this definition because it alleges that Samourai, a money transmitting business operated and controlled by the defendants in whole or in part, charged fees to transfer bitcoin on behalf of its customers from one bitcoin address to another by conducting a series of transactions on the blockchain that Samourai executed and controlled. The Indictment alleges that “Rodriguez and Hill owned, controlled, managed, and supervised Samourai, which was engaged in the business of transferring funds, in the form of bitcoin, on behalf of the public.”⁷ (Ind. ¶ 9). In exchange for a fee, Samourai executed two types of transactions that constituted funds transfers—Whirlpool and Ricochet—which were both designed to conceal the sources and the owners of bitcoin in the

⁶ The defendants do not dispute that Samourai was a business. They dispute only whether Samourai was a business engaged in money transmitting, as opposed to a business engaged in offering privacy software for bitcoin users that did not itself engage in money transmitting.

⁷ The defendants do not dispute that bitcoin constitutes “funds” for the purpose of Section 1960. Nor do the defendants dispute that Samourai offered its services to the public. Instead, the defendants dispute the nature of the service Samourai sold its customers—whether it was purely a privacy service or also a money transmitting service.

transactions. (Ind. ¶¶ 9, 10). To conduct these transactions, “Samourai operated a centralized coordinator server (the ‘Coordinator Server’), managed by Rodriguez and Hill, that, among other things, supervised, executed, and facilitated transactions between Samourai users, and to do so, Samourai created new BTC addresses to which Samourai sent users’ BTC.” (Ind. ¶ 9). In other words, it is the defendants’ business—Samourai—that executed the various transactions described below, which entailed the movement of cryptocurrency between and amongst various addresses created by the business, and it is the defendants that designed, operated, and controlled this business.

In a Whirlpool transaction, a Samourai user “selected an amount of BTC that they wished to mix,” “Samourai ‘cut down’ the cryptocurrency into the correct sizes for the chosen pool” (*i.e.*, divided the bitcoin into the correctly sized input), “Samourai’s Coordinator Server randomly selected four other inputs . . . to be mixed with the new incoming input,” and “[t]he Samourai application on each user’s cellphone then broadcasted a transaction to the blockchain in which all five inputs (each a separate address) were then transferred to five outputs (each a separate address).” (Ind. ¶¶ 16(a)-(b)). “Samourai’s Coordinator Server automatically generated the new addresses that were used as inputs and outputs throughout the process on behalf of users,” thereby transferring users’ bitcoin to new addresses on the blockchain to execute Whirlpool transactions. (Ind. ¶ 16(b)). “[A]fter the mix was complete, Samourai continued to automatically mix the outputs with other batches of cryptocurrency that were in the same pool indefinitely as new cryptocurrency entered the pool, until a user chose to remove their cryptocurrency from the Whirlpool.” (Ind. ¶ 16(c)). “All of these transactions were coordinated by Samourai’s Coordinator Server.” (Ind. ¶ 16(c)).

The defendants designed Ricochet “to build in additional and unnecessary intermediate transactions (known as ‘hops’) on behalf of Samourai users in order to further obscure the source and ownership of funds when Samourai users sent cryptocurrency from one address to another address” on the blockchain. (Ind. ¶ 17). In a Ricochet transaction, “a Samourai user selected an amount of BTC that they wished to send, and the destination address where it was to be sent,” “[t]he Samourai application then created the series of BTC transactions for each Ricochet, including the creation of new addresses, which were transmitted to Samourai’s Coordinator Server,” and “Samourai’s Coordinator Server was responsible for broadcasting the Ricochet transactions to the BTC network.” (Ind. ¶ 18).

In other words, in both Whirlpool and Ricochet transactions, Samourai, using the Coordinator Server controlled by the defendants, transferred users’ bitcoin from one bitcoin address to another, *i.e.*, from one location on the blockchain to another. This type of service to customers is no different from other cryptocurrency mixing services that courts have deemed money transmitting services. As the court explained in *Murgio*, “if the evidence at trial demonstrates that [the alleged money transmitting business] transmitted bitcoin to another location or person for its customers, then that evidence would establish that [the business] was a money transmitting business.” 209 F. Supp. 3d at 711; *see also Roman Storm*, No. 23 Cr. 430 (KPF), ECF No. 84 (Tr. at 22) (indictment adequately alleged a violation of Section 1960 when it alleged that the non-custodial cryptocurrency mixing service Tornado Cash “allowed customers to send cryptocurrency from one wallet to another, without an obvious link between the two wallets, by pooling the customers’ funds in an intermediary wallet on the blockchain, and without necessitating direct customer interaction with Ethereum [a type of cryptocurrency]”); *Harmon*, 474 F. Supp. 3d at 103 (indictment adequately alleged a violation of Section 1960 when it alleged

that the business “enabled customers, for a fee, to send bitcoins to designated recipients in a manner which was designed to conceal and obfuscate the source or owner of the bitcoins” and alleged that the “transaction [conducted by the business] sent bitcoin from an address . . . to another address”; *United States v. Sterlingov*, 573 F. Supp. 3d 28, 31 (D.D.C. 2021) (applying Section 1960 to cryptocurrency mixer that advertised that it could “eliminate any chance of finding your payments[,] . . . making it impossible to prove any connection between a deposit and a withdraw[al] inside our service”). That is exactly what the Samurai service did on behalf of its customers in both Whirlpool and Ricochet transactions.

In seeking to dismiss Count Two, the defendants take an overly narrow view of money transmitting that lacks support in the law. Indeed, “Section 1960 defines ‘money transmitting’ broadly.” *Banki*, 685 F.3d at 113; *E-Gold, Ltd.*, 550 F. Supp. 2d at 88; *Harmon*, 474 F. Supp. 3d at 101; *United States v. Wellington*, No. 1:21-CR-00853-WJ, 2022 WL 3345759, at *7 (D.N.M. Aug. 12, 2022). This is because, “from its inception”, Section 1960 “sought to prevent innovative ways of transmitting money illicitly.” *Murgio*, 209 F. Supp. 3d at 708. “Congress designed the statute to keep pace with such evolving threats, which is precisely why it drafted the statute to apply to any business involved in transferring ‘funds . . . by any and all means.’” *Faiella*, 39 F. Supp. 3d at 546 (quoting 18 U.S.C. § 1960(b)(2)); *Storm*, No. 23 Cr. 430 (KPF), ECF No. 84 (Tr. at 23) (rejecting defendant’s argument that cryptocurrency mixing service was not a money transmitting service because accepting the argument “would frustrate the purpose of Section 1960, which was designed to ‘keep pace with . . . evolving threats’ as new methods of moving criminal proceeds emerged over time” (quoting *Faiella*, 39 F. Supp at 546)).

The defendants define money transmitting restrictively (and incorrectly) by arguing that “transferring” funds requires transferring funds from one third party to a different party who is not

the payor of the funds. (Dkt. 107 at 10-11). To transfer funds, however, does not require that the funds be transferred between two different parties. To transfer funds includes transferring funds from one location to another. For instance, in the very definition cited by the defendants, the word “transfer” means “to convey from one person, place, *or* situation to another.” (Dkt. 107 at 10 (emphasis added) (citing *Transfer*, Merriam-Webster, <https://bit.ly/4mJknA3>)). It is logical that transferring funds does not require transferring funds between different parties. In the context of traditional money transmitting, *i.e.*, transfers of fiat currency by businesses like Western Union or a bank, transfers from one account to another account, even when held by the same person, constitutes transferring funds.

In various cases, courts have held that transferring bitcoin on behalf of others to another location, *i.e.*, to another location on the blockchain, satisfies the definition of money transmitting in Section 1960(b)(2), even where the bitcoin is transferred to the payor at another location. *See, e.g., United States v. Goklu*, No. No. 19 Cr. 386 (PKC), 2023 WL 184254, at *5 n.7 (E.D.N.Y. Jan. 13, 2023) (“The Court notes that even had it considered Defendant’s argument that money transmitting under Section 1960 requires a transfer to a ‘third party’ who is not the payor of funds, it would have rejected it.”); *Storm*, No. 23 Cr. 430 (KPF), ECF No. 84 (Tr. at 22) (indictment adequately alleged a violation of Section 1960 when it alleged that the cryptocurrency mixing service Tornado Cash “allowed customers *to send cryptocurrency from one wallet to another*, without an obvious link between the two wallets, by pooling the customers’ funds in an intermediary wallet on the blockchain, and without necessitating direct customer interaction with Ethereum [a type of cryptocurrency]”) (emphasis added); *Harmon*, 474 F. Supp. 3d at 107 (comparing how traditional money transmitters transfer funds “not by effecting a physical move, but as altering the records in the bank’s ledger system” with how cryptocurrency is transferred,

and concluding “[t]ransferring funds from one bitcoin address to another is as much a transmission between locations”); *United States v. Stetkiw*, No. 18 Cr. 20579 (VAR), 2019 WL 417404, at *2 (E.D. Mich. Feb. 1, 2019) (Bitcoin exchange service, which *transferred bitcoin to the virtual accounts of the bitcoin purchasers*, was engaged in money transmitting pursuant to Section 1960(b)(2)) (emphasis added); *Murgio*, 209 F. Supp. 3d at 711 (“[I]f the evidence at trial demonstrates that [the alleged money transmitting business] *transmitted bitcoin to another location or person* for its customers, then that evidence would establish that [the business] was a money transmitting business.”) (emphasis added). Thus, Samourai, controlled by the defendants, transferred funds by transferring its customers’ bitcoin from one location on the blockchain to multiple other locations on the blockchain in a series of transactions Samourai controlled.

This Circuit’s case law does not compel a different conclusion. The defendants cite the Second Circuit’s description of a money transmitting business as a business that “receives money from a customer and then, for a fee paid by the customer, transmits that money to a recipient in a place that the customer designates.” (Dkt. 107 at 10 (citing *United States v. Velastegui*, 199 F.3d 590, 592 (2d Cir. 1999)). But the quoted language was not a holding of the court; rather, it was in the section of the opinion labeled “background,” in which the court provided an overview of the facts of that particular case. *See* 199 F.3d at 592. For this reason, a court in this district recently observed that this language from *Velastegui* was “dicta” and denied a defendant’s motion to dismiss a Section 1960 charge on the basis that his business did not meet the description in *Velastegui*. *United States v. Neumann*, No. 21 Cr. 439 (NSR), 2022 WL 3445820, at *6-7 (S.D.N.Y. Aug. 17, 2022). The court in *Neumann* recognized that the statutory definition of money transmitting plainly encompasses a broader range of conduct than the background description of the facts in *Velastegui*. *Id.*; *see also Goklu*, 2023 WL 184254, at *5 n.7 (“There is

no indication in *Velastegui* or any other decision, that this explanation, which appears in the ‘Background’ section of *Velastegui*, was intended to define the universe of conduct that qualifies as money transmitting under Section 1960.”⁸

The defendants further argue that Samourai was not a money transmitting business because Samourai, which did not have customers’ private keys, did not take custody of customers’ bitcoin.⁹ (Dkt. 107 at 2, 3, 11). As described above, private keys are akin to a PIN or password that allows a user the ability to access and transfer value associated with the bitcoin address. Custody of the funds, however, is not a requirement to being a money transmitter under Section 1960. Custody is not part of the statute, and the defendants do not cite any case or other legal authority that has ever held that custody of the funds is required.¹⁰ To the contrary, courts have held that control of

⁸ In support of their argument regarding the meaning of “transfer,” defendants cite a case from the Commonwealth Court of Pennsylvania interpreting Pennsylvania’s Money Transmitter Act. (Dkt 107 at 10 (quoting *Givelify LLC v. Dep’t of Banking and Sec.*, 210 A.3d 393, 401-02 (Pa. Commw. Ct. 2019))). Because that case makes no mention of 18 U.S.C. § 1960 and does not interpret that statute, the case is plainly inapposite.

⁹ For support, the defendants rely in part on a letter from two members of Congress to U.S. Attorney General Merrick Garland, which states “non-custodial crypto service providers cannot be classified as money transmitter businesses because users of such services retain sole possession and control of their crypto assets.” (Dkt. 107 at 11) (quoting Letter from Senators Lummis & Wyden to U.S. Attorney General Merrick Garland (2024)). This letter has neither legal authority nor is its reasoning persuasive, for it relies entirely on Section 5330 of the Bank Secrecy Act and FinCEN guidance, neither of which is applicable to the conduct charged here for the reasons described above.

¹⁰ In support, defendants quote a working paper written by lawyers who work for two companies in the cryptocurrency industry. (Dkt. 107 at 11 (Daniel Barabander et al., *Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability for Unlicensed Money Transmitting Businesses Under Section 1960*, Int’l Acad. of Fin. Crim Litigators (2024) (“surveying caselaw and ‘not identify[ing] a single . . . case where a party was ‘money transmitting’ under Section 1960 and did not obtain and relinquish control over funds”))). However, as noted above, courts have held that control of the funds is not a requirement for money transmitting under Section 1960.

the funds is not a requirement for money transmitting under Section 1960. *See Storm*, No. 23 Cr. 430 (KPF), ECF No. 84 (Tr. at 21, 22)¹¹ (“[C]ontrol is not a necessary requirement of the Section 1960 offense” . . . “At its core, the Section 1960 offense seeks to prevent the unlicensed transmission of customer funds from one location to another, *irrespective of whether the transmitter obtained temporary control over the funds to effectuate the transfers* or constructed the transfers specifically in a manner to avoid such control”) (emphasis added); *United States v. Klimenka*, No. 22-CR-00256-SI-1, 2024 WL 4844797, at *3 (N.D. Cal. Nov. 19, 2024) (denying motion to dismiss indictment charging a violation of Section 1960 where the defendant “argues that an indictment must specify in detail the particular control that makes up an alleged violation of Section 1960[,] but he cites no case law in support of this rule”). Rather, as the statutory language dictates, the concept of control is relevant only with respect to the defendant’s association with a money transmitting business. 18 U.S.C. § 1960 (“Whoever knowingly . . . *controls* . . . all or part of an unlicensed money transmitting business shall be fined or imprisoned for not more than 5 years, or both.”). Noticeably absent from the statute are conditions or requirements regarding how that business performs the transmission or transfer of funds from one person or location to another person or location, let alone any requirement that the defendant or the business have “custody” over the funds being transferred for transmitted.

¹¹ The defendants seek to distinguish this decision regarding Tornado Cash by Judge Failla. (Dkt. 107 at 17-18). The defendants argue that because Samourai’s mixing used CoinJoin technology and Tornado Cash did not, Judge Failla’s opinion is not persuasive here. (Dkt. 107 at 17). The opinion, however, is persuasive because neither Samourai nor Tornado Cash took custody of their customers’ cryptocurrency, and the key issue in dispute in both cases is whether a cryptocurrency service provider can transfer funds if it does not take custody of cryptocurrency but nevertheless transfers the cryptocurrency to different locations on the blockchain. Judge Failla held such a cryptocurrency service can qualify as a money transmitting business under Section 1960. *Storm*, No. 23 Cr. 430 (KPF), ECF No. 84 (Tr. at 21, 22).

To be sure, in many or most cases, a money transmitter will take control of the funds that it is transmitting, and it is unsurprising that in many prior cases when courts have described the facts of the particular business at issue, it appears that those businesses did take such control. But it would invite absurd results to hold that because many or most money transmitting businesses have control over the funds while transferring them, there is an unspoken statutory requirement that the business must have control over the funds to be a money transmitter. *See Lomax v. Ortiz-Marquez*, 140 S. Ct. 1721, 1725 (2020) (a court “may not narrow a provision’s reach by inserting words Congress chose to omit”); *Bates v. United States*, 522 U.S. 23, 29 (1997) (“[W]e ordinarily resist reading words or elements into a statute that do not appear on its face.”). If Congress had intended that control of the funds was a requirement, it could have said as much in the plain text of the statute. This is yet another indication that Congress did not implicitly include a “control” or “custody” requirement with respect to the funds in the definition of “money transmitting.”

Samourai is an example, in the bitcoin context, of a money transmitting business that transferred funds without having direct custody of the funds. As the Indictment alleges, “Samourai operated a centralized coordinator server (the ‘Coordinator Server’)” that, among other things, “supervised, executed, and facilitated transactions between Samourai users, and to do so, Samourai created new BTC addresses to which Samourai sent users’ BTC.” (Ind. ¶ 9). Thus, the Indictment alleges that it was Samourai—and not Samourai’s users as the defendants argue—that conducted the transfers of bitcoin.¹² The Government will introduce expert testimony at trial

¹² The defendants argue the Indictment alleges “users—not Samourai or its providers—transmitted their own cryptocurrency and simply used the app to maintain the privacy of their financial transactions.” (Dkt. 107 at 11, 17). This mischaracterizes the allegations in the Indictment. As described above on pages 21-23, the Indictment describes in detail how Samourai, using the Coordinator Server, conducted and controlled the transfer of its users’ bitcoin through

showing how the technology developed by the defendants enabled Samourai to transfer its customers' bitcoin to different locations on the blockchain even though Samourai did not have custody of customers' private keys.

Courts have repeatedly confronted arguments by defendants in similar cases that Section 1960 does not apply to a new technology for transferring funds and have recognized that these arguments would undermine congressional intent. This is because “[f]rom its inception . . . , § 1960 sought to prevent innovative ways of transmitting money illicitly. . . . Congress ‘designed the statute to keep pace with . . . evolving threats,’ and this Court must accordingly give effect to the broad language Congress employed—namely, that § 1960 ‘appl[ies] to *any* business involved in transferring funds . . . by *any and all means*.” *Murgio*, 209 F. Supp. 3d at 708 (quoting *Faiella*, 39 F. Supp. 3d at 546) (emphasis in original).

4. The Defendants’ Due Process Argument Regarding Count Two Is Meritless

Principles of due process require “fair warning . . . in language that the common world will understand” as to the conduct prohibited by law. *McBoyle v. United States*, 283 U.S. 25, 27 (1931). “There are three related manifestations of the fair warning requirement”: the vagueness doctrine; the rule of lenity, which “ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered”; and a bar on courts “applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope.” *United States v. Lanier*, 520 U.S. 259, 266 (1997).

Whirlpool and Ricochet. Moreover, Samourai users only transmitted their own cryptocurrency in the sense that they initiated Whirlpool or Ricochet transactions, including deciding how much bitcoin they wanted to send through the Whirlpool or Ricochet. In much the same way, a bank customer transmits their own fiat currency by initiating a wire transfer on their online bank account, including deciding how much they want to send via wire. But in neither scenario is the *user* the transmitter of the funds—Samourai and the bank transmit the funds.

The defendants challenge Count Two based on the latter two manifestations. (Dkt. 107 at 14-16). The defendants' assertions are groundless; as applied here, neither of the two doctrines comes close to mandating dismissal of Count Two.

The rule of lenity “ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered,” while “due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope.” *Lanier*, 520 U.S. at 266. Neither principle supports dismissal here. The defendants make no showing at all as to how 18 U.S.C. § 1960 is ambiguous.¹³ Indeed, as discussed above, the terms of the statute are plain and straightforward. The mere fact that a defendant can put forward a cramped reading of a statute does not give rise to the rule of lenity if the best reading of the statute extends to his conduct. *See Pulsifer v. United States*, 601 U.S. 124, 152 (2024) (improper to invoke rule of lenity merely because there are multiple “permissible readings of the statute when viewed in the abstract”); *E-Gold*, 550 F. Supp. 2d at 100 (rule of lenity is reserved for “those situations in which a reasonable doubt persists about a statute’s intended scope even *after* resort to ‘the language and structure, legislative history, and motivating policies’ of the statute”) (quoting *Moskal v. United States*, 498 U.S. 103, 108 (1990)) (emphasis in original).

The defendants’ novel construction argument is equally unavailing. While a statute must give a defendant fair notice that his conduct is unlawful, as the statute at issue here plainly does,

¹³ The defendants indirectly seek to support their motion by citing a memorandum dated April 7, 2025, “Ending Regulation by Prosecution,” by the Deputy Attorney General. The memorandum states on its face that it “is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.” Accordingly, the Court should not consider this memorandum.

there is no requirement that there have been “a factual situation that is ‘fundamentally similar’” to the crime charged. *Lanier*, 520 U.S. at 269; *Ponnapula v. Spitzer*, 297 F.3d 172, 183 (2d Cir. 2002) (“Due process is not, however, violated simply because the issue is a matter of first impression.”). As discussed above, the defendants’ alleged conduct is similar to other cryptocurrency businesses in which courts have rejected similar challenges to unlicensed money transmitting charges. Samourai is at least the fifth different cryptocurrency mixing service to be prosecuted by the Department of Justice for money laundering and violating Section 1960 since 2020. See *United States v. Storm*, No. 23 Cr. 430 (KPF), Dkts. 83 (order denying motion to dismiss charges against “Tornado Cash” cryptocurrency mixing service), 84 at 15-46 (transcript of oral order denying motion to dismiss); *Sterlingov*, 573 F. Supp. 3d at 30 (“Bitcoin Fog is a bitcoin mixer (or tumbler) that offers further anonymity to those engaged in bitcoin transactions. . . . [T]he service enables them ‘to send bitcoins to designated recipients in a manner designed to conceal and obfuscate the sources of the bitcoins.’”); *Harmon*, 474 F. Supp. 3d at 99 (“Helix enabled customers, for a fee, to send bitcoins to designated recipients in a manner which was designed to conceal and obfuscate the source or owner of the bitcoins.”); *United States v. Nguyen*, No. 23 Mag. 528 (E.D. Pa. Mar. 14, 2023) (Doc. 1) (criminal complaint and arrest warrant for ChipMixer money laundering service operating as cryptocurrency mixer). To be sure, each of those cases also raised some novel issues when they were brought. That is the inevitable result of the application of longstanding criminal statutes to new technologies. Some case has to be first. *United States v. Ulbricht*, 31 F. Supp. 3d 540, 566 (S.D.N.Y. 2014) (“The fact that a particular defendant is the first to be prosecuted for novel conduct under a pre-existing statutory scheme does not *ipso facto* mean that the statute is ambiguous or vague or that he has been deprived of constitutionally appropriate notice.”); *United States v. Kinzler*, 55 F.3d 70, 74 (2d Cir. 1995)

(“[C]laimed novelty of this prosecution does not help [defendant’s] cause, for it is immaterial that there is no litigated fact pattern precisely in point.”). The defendants’ criminal conduct may not be identical in every respect to similar prior criminal schemes. That, however, does not constitute a due process violation.¹⁴

C. Count One Sufficiently Alleges a Conspiracy to Commit Money Laundering

Rodriguez and Hill also move to dismiss Count One of the Indictment, which charges them with participating in a conspiracy to commit concealment money laundering, in violation of 18 U.S.C. § 1956 (h). According to the defendants, the Indictment fails to allege that they had knowledge of any money laundering conspiracy, or that they agreed to join in any such conspiracy. These allegations are completely meritless. Count One of the Indictment tracks the statutory language of 18 U.S.C. §§ 1956(h) and 1956(a)(1)(B)(i) and adequately alleges the elements and approximate dates of the offense, thereby informing the defendants of the charges and permitting them to plead a Double Jeopardy claim in the future. For this reason alone, the motion to dismiss Count One should be denied, and any arguments about defendants’ criminal intent should be decided at trial. In any event, the Indictment charges Rodriguez and Hill with intentionally designing, marketing, and operating Samourai as a cryptocurrency mixing service to be used by criminals to launder their crime proceeds. On multiple occasions, Rodriguez and Hill even specifically solicited certain types of criminals to engage in money laundering using Samourai, including darknet marketplace users, hackers, and sanctions evaders. If proven at trial, these

¹⁴ The defendants primarily rely on historical FinCEN guidance to argue that this prosecution is a novel construction of Section 1960 in violation of due process. (Dkt. 107 at 15). For all the reasons described above, *see supra* at 15-19, nn. 2, 5, and *infra* 71, 75-76 & n.20, FinCEN’s guidance is irrelevant because Section 1960(b)(1)(B), concerning failure to register as a money transmitting business with FinCEN, is no longer charged.

allegations are more than sufficient for Rodriguez and Hill to be convicted of knowingly participating in a money laundering conspiracy.¹⁵

1. The Indictment Tracks the Statutory Language of Sections 1956(h) and 1956(a)(1)(B)(i) and Fairly Informs the Defendants of the Charge

At the outset, Rodriguez and Hill’s motion to dismiss Count One should be denied because the Indictment “track[s] the language of the statute charged and state[s] the time and place (in approximate terms) of the alleged crime.” *Dawkins*, 999 F.3d at 779. The Indictment also adequately provides notice to Rodriguez and Hill of the elements of the offense charged, fairly informs them of the charge against which they must defend, and enables them to plead an acquittal or conviction in bar of future prosecutions for the same offense. *Id.* (quoting *Wedd*, 993 F.3d at 120). Beyond providing notice of the charge, the Indictment also includes numerous details about the factual nature of the charge, with over 20 pages worth of factual allegations regarding how Samourai functioned, Rodriguez and Hill’s statements and actions demonstrating their participation in the money laundering conspiracy, as well as a host of specific examples of criminal proceeds that were laundered through Samourai, including proceeds from the Silk Road and Hydra darknet markets, and multiple hacks and fraud schemes. Rodriguez and Hill have not raised any challenges to being adequately provided notice of the charge in the Indictment.

¹⁵ Rodriguez and Hill also argue that Count One must be dismissed because Samourai was not a “financial institution” under 18 U.S.C. § 1956(c)(4)(B). This argument is now moot because the S3 Superseding Indictment does not allege that Samourai was a “financial institution” under § 1956(c)(4)(B). Instead, Count One now alleges that Samourai engaged in transactions affecting interstate or foreign commerce “involving the movement of funds by wire or other means” for purposes of 18 U.S.C. § 1956(c)(4)(A). As a result, the Court no longer needs to determine whether Samourai constitutes a “financial institution” under 31 U.S.C. § 5312(a)(2), which is now moot.

Nothing more is required at this stage of the proceedings, and any further evaluation of the adequacy of the facts to satisfy the elements of Count One should be reserved for trial. *Dawkins*, 999 F.3d at 780 (“But at the indictment stage, we do not evaluate the adequacy of the facts to satisfy the elements of the charged offense. That is something we do after trial. Otherwise, we would effectively be asking district courts to engage in summary judgment proceedings—something that does not exist in federal criminal procedure.” (quoting *Wedd*, 993 F.3d at 120)). To the extent that Rodriguez and Hill are making claims about their lack of specific intent to engage in a money laundering conspiracy, this is a paradigmatic factual dispute that the Second Circuit has held must be resolved at trial. *See United States v. Sampson*, 898 F.3d 270, 281 (2d Cir. 2018) (“But when a defense raises a factual dispute that is inextricably intertwined with a defendant’s potential culpability, a judge cannot resolve that dispute on a Rule 12(b) motion.”); *id.* (“[T]he Supreme Court has admonished that where intent of the accused is an ingredient of the crime charged, its existence is a question of fact that a judge cannot resolve on the jury’s behalf.” (quoting *Morissette v. United States*, 342 U.S. 246, 274 (1952))); *United States v. Percoco*, No. 16 Cr. 776 (VEC), 2017 WL 6314146 at *7 (S.D.N.Y. Dec. 11, 2017) (“[T]he sufficiency of the Government’s evidence of intent cannot be considered on a motion to dismiss the indictment, and the indictment need only track the language of the statute.”) (citing *United States v. Martin*, 411 F. Supp. 2d 370, 373 (S.D.N.Y. 2006)). At trial, the Government intends to prove that Rodriguez and Hill willfully and knowingly participated in a money laundering conspiracy, agreeing with each other and with their customers to conceal the proceeds of criminal activity through Samourai. At that time, the defendants will have a full and fair opportunity to argue to the jury why they believe the Government’s evidence is insufficient. For this reason alone, the motion to dismiss Count One should be denied, and the parties should proceed to trial, where Rodriguez and Hill will

have ample opportunity to argue that they lacked the specific knowledge and intent to be found guilty on Count One.

2. The Indictment Properly Alleges a Conspiracy to Commit Money Laundering

As discussed above, the Court should not entertain Rodriguez and Hill's motion to dismiss Count One, given that it is premised on "predictions as to what the trial evidence will be" regarding their knowledge and intent about Samurai's nexus with money laundering. *Sampson*, 898 F.3d at 285. Nonetheless, by its own terms, Rodriguez and Hill's motion to dismiss fails because it misstates the applicable law relating to money laundering conspiracies, and it misunderstands the allegations in the Indictment, including the evidence that the Government will present at trial relating to Rodriguez and Hill's knowledge and intent to engage in large scale money laundering using Samurai.

To begin with, Rodriguez and Hill incorrectly suggest that a money laundering conspiracy requires proof that they "agree[d] to join any customer's conspiracy" or that they "knew of particular instances of misuse of the app by any customer or that Samurai Wallet transactions by users involved the proceeds of a crime." (Docket No. 95 at 36-37). These arguments completely misunderstand the law that applies to money laundering conspiracies, and conspiracies more broadly. Section 1956(h) makes it a crime to "conspire[] to commit *any offense defined in this section*" (emphasis added). "Conspiring to launder money requires that two or more people agree to violate *the federal money laundering statute*, and that the defendant knowingly engaged in the conspiracy with the specific intent to commit the offenses that are the objects of the conspiracy." *United States v. Garcia*, 587 F.3d 509, 515 (2d Cir. 2009) (emphasis added). As the Second Circuit explained over 30 years ago:

Section 1956 creates the crime of money laundering, and it takes dead aim at the attempt to launder dirty money. Why and how that money got dirty is defined in other statutes. Section 1956 does not penalize the underlying unlawful activity from which the tainted money is derived....[T]he particular underlying activity specified by Congress is a necessary, but ancillary, concern....[T]he focal point of the statute is the laundering process, not the underlying unlawful conduct that soiled the money.

United States v. Stavroulakis, 952 F.2d 686, 691 (2d Cir. 1992) (emphasis omitted).

“Significantly, an individual need not have been convicted of the underlying criminal offense in order to be convicted of laundering the proceeds thereof.” *United States v. Silver*, 948 F.3d 538, 576 (2d Cir. 2020) (emphasis omitted); *see also United States v. Neuman*, 621 F. App’x 363, 365-66 (9th Cir. 2015) (“[A] defendant does not have to commit or be convicted of the underlying substantive specified unlawful activity that generated the illegal proceeds to be guilty of a conspiracy to commit money laundering.”) (emphasis omitted).

Importantly, the money laundering statutes also do not require that defendants have specific knowledge of the particular crime from which the proceeds were derived. Rather, the charged § 1956 offense merely requires that a defendant know that funds involved in the money laundering transaction are “proceeds of *some form* of unlawful activity.” 18 U.S.C. § 1956(a)(1) (emphasis added); *see United States v. Maher*, 108 F.3d 1513, 1526 (2d Cir. 1997) (explaining that the “clear intent” of § 1956(a)(1) is to “reach a person who knows that he is dealing with the proceeds of ‘some’ crime even if he does not know precisely which crime”). In *Stavroulakis*, the Second Circuit went even further and held that in a money laundering conspiracy, the specified unlawful activity at issue is “ancillary” and therefore, “it is not essential” that two money laundering co-conspirators even “agree on the same illegal activity” for which they are agreeing to launder proceeds. 952 F.2d at 690-91. Similarly, courts have held that a jury does not need to reach

“unanimity as to which specified unlawful activity or activities triggered the violation of the statute” *United States v. Aguilar*, 742 F. Supp. 3d 322, 345 (E.D.N.Y. 2024).

Based on this well-established law, the Government need not prove at trial that Rodriguez and Hill had reached a “meeting of the minds” with any particular customers seeking to use Samourai for money laundering, or that they were aware of any ongoing money laundering transactions that were occurring in real time. Rather, an agreement between Rodriguez and Hill that they would use Samourai to engage in money laundering transactions on behalf of its customers is enough, even if no customers ever ended up joining the conspiracy or actually sent criminal proceeds to Samourai to be laundered. *See United States v. Svoboda*, 347 F.3d 471, 476 (2d Cir. 2003) (“The gist of conspiracy is, of course, agreement.” (quoting *United States v. Beech-Nut Nutrition Corp.*, 871 F.2d 1181, 1191 (2d Cir. 1989)); *United States v. Jimenez Recio*, 537 U.S. 270, 274-75 (2003) (“The Court has repeatedly said that the essence of a conspiracy is an agreement to commit an unlawful act . . . That agreement is a distinct evil, which may exist and be punished whether or not the substantive crime ensues.” (internal citations omitted)). Because Rodriguez and Hill are merely being charged with conspiracy, a “financial transaction involving the proceeds of specified unlawful activity is an element of the underlying object of the conspiracy, but not an element of the conspiracy itself.” *United States v. Shea*, No. 20 Cr. 412 (AT), 2023 WL 4551635, at *3 (S.D.N.Y. July 14, 2023); *see also Stavroulakis*, 952 F.2d at 691 (rejecting the argument that “the particular specified unlawful activity is an essential element of the crime”); *United States v. Paldiel*, No. 24 Cr. 329 (ARR), 2025 WL 524659, at *13 (E.D.N.Y. Feb. 18, 2025) (“[B]ecause Mr. Paldiel is charged with conspiracy, the government does not need to prove that the transaction occurred.”); *United States v. Wittig*, 575 F.3d 1085, 1103-04 (10th Cir. 2009) (Gorsuch, J.) (rejecting argument that a conspiracy to launder money must take the form: “Let us

launder *this* money” and explaining that defendants committed conspiracy if they agreed to launder the money they planned to obtain in the future from a wire fraud scheme). As a result, Rodriguez and Hill are wrong to suggest that a money laundering conspiracy charge requires that they “knew of these transactions” or the “reason for these transactions” in real time. (Docket No. 95 at 37). Rather, the Government does not need to prove that *any* transactions ultimately occurred at all, as long as there was an agreement to commit money laundering.¹⁶

Additionally, the Government has charged numerous money laundering networks and money laundering services with participating in a criminal conspiracy on analogous fact patterns—defendants agreeing with one another to provide a service for criminals to engage in the transfer of tainted funds without detection by law enforcement. *See, e.g., United States v. Fares*, 95 F. App’x 379, 382 (2d Cir. 2004) (defendant convicted of participating in Black Market Peso Exchange by receiving with her cousin over \$7 million in small bills “from a number of different people, some of whom they did not know” and depositing them into bank accounts); *United States v. Weiner*, 152 F. App’x 38, 40 (2d Cir. 2005) (finding that Weiner and co-defendant had a “meeting of the minds” to offer money laundering services to the undercover agents); *see also United States v. Gamez*, 1 F. Supp. 2d 176, 181 (E.D.N.Y. 1998) (“Those ‘washing’ money frequently have not engaged directly in the criminal action that dirtied the cash.”). Simply put, Rodriguez and Hill’s agreement with each other to violate 18 U.S.C. § 1956 by providing money laundering services to criminals is sufficient to sustain a conviction as to Count One.

¹⁶ As such, because a conspiracy can be accomplished by two people who merely agree to commit a crime, the Second Circuit has upheld criminal conspiracy charges where a group of defendants conspired to sell illegal arms to undercover agents, *see, e.g., United States v. Al Kassir*, 660 F.3d 128-29 (2d Cir. 2011), as well as conspiracy charges where the objectives of the conspiracy were impossible or unattainable from the outset, *see United States v. Wallace*, 85 F.3d 1063, 1068 (2d Cir. 1996) (collecting cases).

Similarly, Rodriguez and Hill incorrectly suggest that the evidence at trial will merely show that “they knew generally that some people could use the app to commit crimes and that they did not employ various [Anti-Money Laundering] programs and procedures to stop it.” (Docket No. 95 at 41). Quite to the contrary, as reflected in the Indictment, the Government’s proof at trial will include evidence that Rodriguez and Hill agreed with each other that Samourai would proactively offer and supply money laundering services to its customers. For example, Samourai actively marketed its money laundering services to users of darknet marketplaces, and the defendants were “entirely focused on . . . black/grey markets” and “Restricted Markets” like the Silk Road and Hydra. (Ind. at ¶¶ 21-23, 30, 32). The defendants also personally encouraged hackers to “[f]eed” and [s]end” the proceeds of a July 2020 hack of a social media company into their platform, even enticing the hackers with a 20% discount on all Whirlpool fees. (Ind. at ¶ 25). Additionally, even though proof of their specific knowledge as to particular criminal proceeds is not necessary, the Government’s proof at trial will include text messages from February 19, 2024, when Hill was placed on notice that Samourai was being used to launder the proceeds of a well-publicized hack of \$26 million from a decentralized cryptocurrency exchange. (Ind. ¶ 37). Similarly, Rodriguez bragged in September 2019 about how Iran, a country subject to U.S. sanctions, was the second largest country of Samourai downloads after the United States, and he followed up with a message in December 2020 actively encouraging users from Iran to “run their BTC acquired via Iranian exchanges in Whirlpool”—a thinly-veiled reference to the fact that Iranian exchanges are sanctioned entities under IEEPA. (Ind. ¶ 28). This evidence of intent shows that the Government is not seeking to merely hold Rodriguez and Hill vicariously liable for crimes committed by their customers that occurred without their knowledge or consent. Rather, Rodriguez and Hill actively solicited, encouraged, desired, and agreed with each other to launder

criminal proceeds of others through Samourai, and their efforts had the intended effect, with millions of dollars of crime proceeds being laundered through Samourai.

Finally, Rodriguez and Hill heavily rely on several cases where courts have cautioned the Government about expanding conspiratorial or aiding and abetting liability to businesses that merely provide an innocent product or service to customers, who may choose to abuse the product or service to commit crimes. *See, e.g., United States v. Falcone*, 311 U.S. 205, 211 (1940) (supplier of sugar, yeast, and cans who “without more furnishes supplies to an illicit distiller is not guilty of conspiracy even though his sale may have furthered the object of a conspiracy to which the distiller was a party but of which the supplier had no knowledge”); *United States v. Superior Growers Supply, Inc.*, 982 F.2d 173, 178 (6th Cir. 1993) (“Absent an awareness that their customers are manufacturing marijuana, defendants [suppliers of gardening equipment] cannot have the requisite criminal intent to conspire to aid and abet them.”).

But Rodriguez and Hill ignore the large body of cases that have distinguished *Falcone* and *Superior Growers Supply*, especially in cases like this one where the defendants intended their business to serve as a conduit for laundering, or where the business is clearly on notice that their products have a high potential for abuse by criminals. *See, e.g., Direct Sales Co. v. United States*, 319 U.S. 703, 710 (1940) (upholding conspiracy conviction for supplier of morphine sulphate); *United States v. Zambrano*, 776 F.2d 1091, 1095 (2d Cir. 1985) (upholding conspiracy conviction for supplier of unembossed credit cards); *United States v. Bondars*, 801 F. App’x 872, 881-83 (4th Cir. 2020) (upholding conspiracy and aiding and abetting convictions for providing a malware scanning service for hackers to see if malware would be detected by anti-virus software). In *Direct Sales*, for example, the Supreme Court pointed out that not all commodities and services are equal in terms of their “inherent capacity for harm and from the very fact they are restricted.”

319 U.S. at 711). As a result, if a seller of opiates attempts to “stimulate such sales by all the high-pressure methods, legal if not always appropriate, in the sale of free commodities” where the “primary effect is rather to create black markets for dope and to increase illegal demand and consumption,” then “there is no legal obstacle to finding the supplier not only knows and acquiesces, but joins both mind and hand with him to make its accomplishment possible.” *Id.* at 712-13. Similarly, the Second Circuit in *Zambrano* laid out a very clear principle regarding conspiratorial liability for suppliers of goods:

Thus, evidence that a defendant simply supplies goods, innocent in themselves, to someone who intended to use them illegally is not enough to support a conviction for conspiracy. But, if there is something more, some indication that the defendant knew of and intended to further the illegal venture, that he somehow encouraged the illegal use of the goods or had a stake in such use, sufficient evidence has been presented to enable the jury to conclude the defendant had knowledge of and an intent to join in the conspiracy.

777 F.2d at 1095; *see also United States v. Orozco-Prada*, 732 F.2d 1076, 1080 (2d Cir. 1984) (holding that the “knowing supply of a raw material necessary for the commission of a crime by another constitutes aiding and abetting that crime”); *Bondars*, 801 F. App’x at 882-83 (rejecting argument that defendant never communicated with Scan4You clients directly because the company “advertised [the service] on hacker forums, advertised malware on the Scan4You website, entered into client agreements with prolific hackers, and expressed fear of criminal prosecution and the need to be discreet”).

This case has similarities to various Silk Road prosecutions, where in one case Judge Forrest approved a charge for conspiracy to commit money laundering based on the allegations that the defendant “purposefully and intentionally designed, created, and operated Silk Road to facilitate unlawful transactions,” that such unlawful transactions in fact took place on Silk Road, and that the defendant “obtained significant monetary benefit in the form of commissions in

exchange for the services he provided via Silk Road.” *United States v. Ulbricht*, 31 F. Supp. 3d 540, 556 (S.D.N.Y. 2014); *see also id.* at 558 (“It is as though the defendant allegedly posted a sign on a (worldwide) bulletin board that said: ‘I have created an anonymous, untraceable way to traffic narcotics, unlawfully access computers, and launder money. You can use the platform as much as you would like, provided you pay me a percentage of your profits and adhere to my other terms of service.’”). It is also analogous to the recent prosecutions of: (1) Roman Storm, who similarly filed a motion to dismiss a money laundering conspiracy charge based on the Tornado Cash cryptocurrency mixer, which was denied by Judge Failla, *see Storm*, No. 23 Cr. 430 (KPF), ECF No. 84 (Tr. at 25-31) (“The government did not have to allege that Mr. Storm conspired with any of Tornado Cash’s users to promote or further any of the illicit purposes of their transactions. Indeed, the government did not have to allege that Mr. Storm was aware of the specific nature, much less be a participant in, the underlying criminal activity.”); and (2) Roman Sterlingov, who created a similar cryptocurrency mixer called Bitcoin Fog and was recently convicted at trial of money laundering conspiracy, *United States v. Sterlingov*, No. 21 Cr. 399 (RDM) (D.D.C.). *See also United States v. Harmon*, No. 19 Cr. 395 (BAH) (D.D.C.), Dkt. 123 (cryptocurrency mixer operator entering statement of offense in connection with guilty plea to money laundering conspiracy). Based on the caselaw described above, Hill and Rodriguez have no basis to argue that the money laundering conspiracy charges in this case are improperly holding them liable for the actions of their customers, or that the charges are otherwise unprecedented or unsupported by basic conspiracy law.

For these reasons, the Court should dismiss Hill and Rodriguez’s motion to dismiss Count One and allow for any factual disputes about their criminal intent to be decided at trial.

II. Hill's Motion to Suppress and Request for a *Franks* Hearing Should Be Denied

Hill moves to suppress all evidence identified during a search of his personal email account (the "HILL Email Account"), which was authorized by the Honorable Gabriel W. Gorenstein, United States Magistrate Judge for the Southern District of New York, in a search warrant issued on March 7, 2023 (attached as Exhibit 2 to Hill's Motion to Suppress). The search warrant was issued based upon a sworn affidavit by FBI Special Agent Yohanna Peña (the "Peña Affidavit", Exhibit 1 to Hill's Motion to Suppress). According to Hill, the search warrant was invalid because: (1) the Peña Affidavit contained false and misleading statements; (2) the Peña Affidavit failed to establish probable cause that evidence of criminal activity would be found in the HILL Email Account; and (3) the search warrant was overbroad and failed to provide meaningful guidance regarding what data could be seized. Hill also argues that the good faith exception does not apply, and he requests that the Government return or destroy the full extraction of the HILL Email Account that the Government received from Hill's email provider. As further discussed below, all of these arguments are meritless, and Hill's motion to suppress should be denied.

A. The Search Warrant Affidavit for Hill's Email Account Contained No False or Misleading Statements that Were Material to Probable Cause

At the outset, Hill argues that the Peña Affidavit contained the following allegedly false and misleading statements or omissions: (1) the suggestion that law enforcement had "not yet identified the individuals who control Samourai's day-to-day operations" (Peña Affidavit ¶ 9(e)); (2) the failure to describe records that had already been obtained from Samourai's electronic business accounts showing that those accounts were being used to actively manage the business; and (3) Special Agent Peña's belief that the HILL Email Account was being "actively used to operate and further Samourai's business" (Peña Affidavit ¶ 9(e)). But none of these statements were false, intentionally or recklessly misleading, or material to Judge Gorenstein's finding of

probable cause that evidence of criminal activity would be found within the HILL Email Account. As a result, Hill’s challenge to the search warrant affidavit and request for a *Franks* hearing should be denied.

1. Applicable Law

a. The *Franks* Standard

“A search warrant affidavit is presumed reliable.” *United States v. Klump*, 536 F.3d 113, 119 (2d Cir. 2008) (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)). “The task of a reviewing court is simply to ensure that the ‘totality of the circumstances’ afforded the [issuing judge] a ‘substantial basis’ for making the requisite probable cause determination.” *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). “In certain circumstances, however, a defendant may challenge the truthfulness of factual statements made in the affidavit, and thereby undermine the validity of the warrant and the resulting search or seizure.” *United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003) (citing *Franks*, 438 U.S. at 164-72). “[A] defendant seeking to suppress evidence obtained pursuant to an affidavit containing erroneous information must satisfy both a state of mind requirement and a materiality requirement by showing that (1) the claimed inaccuracies or omissions are the result of the affiant’s deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge’s probable cause finding.” *United States v. Lauria*, 70 F.4th 106, 126 (2d Cir. 2023); *see also Klump*, 536 F.3d at 119 (“To void the warrant and suppress the evidence based on a defective affidavit, the defendant must demonstrate, by a preponderance of the evidence, that there were intentional and material misstatements or omissions in the search warrant affidavit.”). “The *Franks* standard is a high one.” *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991). “An affiant cannot be expected to include in an affidavit every piece of

information gathered in the course of an investigation.” *United States v. Rajaratnam*, 719 F.3d 139, 154 (2d Cir. 2013). “[M]isstatements or omissions caused by ‘negligence or innocent mistake[s]’ do not warrant suppression.” *Id.* at 153 (quoting *Franks*, 438 U.S. at 171).

b. Intentionality of the False Statements

To find that an affiant intentionally made misstatements or omissions in the search warrant affidavit, the “reviewing court must be presented with credible and probative evidence that the omission of information . . . was ‘designed to mislead’ or was ‘made in reckless disregard of whether [it] would mislead.’” *Id.* at 154 (quoting *Awadallah*, 349 F.3d at 68). A misstatement or omission is intentional only when “the claimed inaccuracies or omissions are the result of the affiant’s deliberate falsehood or reckless disregard for the truth.” *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). “To prove reckless disregard for the truth, the defendant[] must prove that the affiant in fact entertained serious doubts as to the truth of his allegations.” *Rajaratnam*, 719 F.3d at 154; *see also United States v. Falso*, 544 F.3d 110, 126 (2d Cir. 2008) (“Allegations of negligence or innocent mistake are insufficient.” (quoting *Franks*, 438 U.S. at 171)).

Moreover, alleged “[o]missions are not subject to the same high level of scrutiny as misstatements.” *United States v. Rivera*, 750 F. Supp. 614, 617 (S.D.N.Y. 1990). As noted above, “[a]n affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation.” *Awadallah*, 349 F.3d at 67-68. Because “all storytelling involves an element of selectivity,” it is “not shocking that every affidavit will omit facts which, in retrospect, seem significant.” *United States v. Vilar*, No. 05 Cr. 621 (KMK), 2007 WL 1075041, at *27 (S.D.N.Y. Apr. 4, 2007). Thus, “as a practical matter the affirmative inclusion of false information in an affidavit is more likely to present a question of impermissible

official conduct than a failure to include a matter that might be construed as exculpatory.” *United States v. Mandell*, 710 F. Supp. 2d 368, 374 (S.D.N.Y. 2010). This is because “allegations of omission potentially open officers to endless conjecture about investigative leads, fragments of information, or other matter that might, if included, have redounded to defendant’s benefit.” *Id.*

c. Materiality

To determine materiality, courts should “disregard the allegedly false statements,” *Awadallah*, 349 F.3d at 65, “insert the omitted truths,” *Rajaratnam*, 719 F.3d at 146, and determine whether “there remains a residue of independent and lawful information sufficient to support probable cause.” *Awadallah*, 349 F.3d at 65. “If, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a *Franks* hearing.” *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998). “Courts have repeatedly been warned not to interpret the affidavit in a hypertechnical, rather than a commonsense, manner.” *Canfield*, 212 F.3d at 719. In the end, “the defense motion must be denied without a hearing if, after setting aside the allegedly misleading statements or omissions, there remains a residue of independent and lawful information sufficient to support probable cause.” *United States v. Levasseur*, 816 F.2d 37, 43 (2d Cir. 1987).

d. Standard for Evidentiary Hearing

To invoke the *Franks* doctrine and meet the standard for obtaining an evidentiary hearing, the defendant must “make a substantial preliminary showing” that there were intentional misstatements or omissions and the warrant affidavit and that those misstatements or omissions were material. *United States v. McKenzie*, 13 F.4th 223, 236 (2d Cir. 2021). *See Awadallah*, 349 F.3d at 64; *Rajaratnam*, 719 F.3d at 146. To ultimately prevail on a *Franks* challenge, the

defendant must establish both components—*i.e.*, intent and materiality—by a preponderance of the evidence. *See Klump*, 536 F.3d at 119.

2. Discussion

Applying the standards described above, Hill fails at every step of the *Franks* analysis in showing that the Peña Affidavit contained false or misleading statements that render the search warrant invalid:

First, Hill cannot show that any of the alleged statements or omissions were actually false or misleading. To begin with, Hill argues that it was misleading for the Peña Affidavit to suggest that law enforcement officers “have not yet identified the individuals who control Samourai’s day-to-day operations” when law enforcement agents had in fact collected a significant amount of evidence suggesting that Samourai was being operated by Rodriguez and Hill. (Peña Affidavit at ¶ 9(e)). But read in context, there was nothing misleading about this statement at all. In the rest of paragraph 9(e), the Peña Affidavit acknowledges news reports indicating that Rodriguez and Hill were the co-founders of Katana Cyptographic, which was Samourai’s parent company. The Peña Affidavit also indicates that law enforcement agents are “seeking to confirm whether RODRIGUEZ and HILL are controlling Samourai, and to identify any other individuals who are responsible for Samourai’s day-to-day operations.” (Peña Affidavit at ¶ 9(e)). Reading these statements together in context, the Peña Affidavit was not false or misleading at all in identifying Hill as someone who law enforcement was trying to “confirm” as one of the owners and operators of Samourai, while also stating that law enforcement was still trying to identify *any other individuals* who are responsible for Samourai’s day-to-day operations. At this stage in the investigation, Peña was truthfully and accurately stating that law enforcement was still looking for additional evidence confirming Rodriguez and Hill’s connections to Samourai, as well as

identifying any other individuals who might be participating in Samourai's criminal activities.

Similarly, Hill argues that it was false and misleading for the Peña Affidavit to allege that the HILL Email Account was being “actively used to operate and further Samourai's business” (Peña Affidavit ¶ 9(e)), and he argues that the Peña Affidavit should have pointed out that it was the Samourai business email accounts (like `wallet@samouraiwallet.com` and `dev@samouraiwallet.com`) that were used to actively operate Samourai's business because they contained a larger volume of Samourai-related emails. But Hill cannot show that any of these statements or omissions were “designed to mislead,” *Awadallah*, 349 F.3d at 68, or that Special Agent Peña “entertained serious doubts as to the truth of [her] allegations,” *Rajaratnam*, 719 F.3d at 154. As Hill concedes, law enforcement officers took the step of obtaining an 18 U.S.C. § 2703(d) order for the emails in the HILL Email Account, and there were approximately 90 emails between August 6, 2015 and January 14, 2019 that were exchanged between the HILL Email Account and Samourai-related email accounts, like `dev@samouraiwallet.com`, `samouraidev@tuta.io`, `wg@samourai.io`, `tdevd@samourai.is`, and `sam@samourai.io`. (Peña Affidavit ¶ 23(b)). Additionally, there were, between September 13, 2015, and December 19, 2018, emails with other digital currency and business support email accounts, including [REDACTED]@tuta.nota.com (who was also copied on emails from Samourai-domain email accounts), `stashsupport@stashcrypto.com`, [REDACTED]@stashcrypto.com, and `support@wirexzendesk.com`. (*Id.*). Based on the fact that there were emails being exchanged with Samourai-related email addresses and Samourai-related domains, it was not misleading for the Peña Affidavit to allege that the HILL Email Account was being “actively used to operate and further Samourai's business”—especially given that Peña gave very specific details as to the facts she was relying upon to make that assessment. Similarly, the mere fact that

dev@samouraiwallet.com might have been the primary email account used by Hill to conduct Samourai-related business does not mean that Hill's personal email account—the HILL Email Account—might not also have evidence of Hill's participation in Samourai, or that it was not actively used to conduct Samourai-related business. Indeed, even if the HILL Email Account was only periodically being used to conduct Samourai-related business, that would have still provided probable cause for a search of the HILL Email Account. Based on the totality of the Peña Affidavit, there is no evidence that Special Agent Peña was trying to mislead Judge Gorenstein or was otherwise being reckless about the truth. Rather, the Peña Affidavit contained the specific data from the 18 U.S.C. § 2703(d) order that supported Peña's belief that the HILL Email Account would contain evidence of Samourai's business operations and Hill's connections to Samourai. If Judge Gorenstein did not believe that "approximately 90 emails" was sufficient to warrant a probable cause finding, he had every opportunity to deny the warrant on that basis.

Finally, Hill has not even come close to showing that any of the alleged false statements or omissions—whether viewed individually or collectively—were material. Even if the Peña Affidavit had not included all of the allegedly false statements and omissions described above, the Peña Affidavit still would have laid out probable cause that evidence of Hill's participation in Samourai would be found within the HILL Email Account, especially given all the emails exchanged between the HILL Email Account and Samourai-related email addresses. Similarly, given the different Samourai-related email addresses that were communicating with the HILL Email Account—like wg@samourai.io, sam@samourai.io, and [REDACTED]@tuta.nota.com (who was copied on emails from Samourai-domain email accounts), there was probable cause to believe that the HILL Email Account would contain emails that would provide information about other unidentified individuals who were participating in Samourai's criminal activities.

Especially given that the low bar of probable cause only requires a “fair probability that contraband or evidence of a crime will be found in a particular place,” *Illinois v. Gates*, 462 U.S. 213, 214 (1983), there would still be ample probable cause to support the search of the HILL Email Account, even if all of Hill’s alleged misstatements and omissions had been corrected. *See United States v. Nejad*, 436 F. Supp. 3d 707, 722 (S.D.N.Y. 2020) (“Even assuming these affidavits contain errors that require correcting, excising the alleged errors from them only demonstrates the overwhelming strength of the probable cause showing.”).

Because Hill cannot “make a substantial preliminary showing” that there were intentional misstatements or omissions in the warrant affidavit and that those misstatements or omissions were necessary to the finding of probable cause, the Court should deny Hill’s request for a *Franks* hearing. *See McKenzie*, 13 F.4th 223, 236 (2d Cir. 2021).

B. The Search Warrant Affidavit for Hill’s Email Account Was Supported by Ample Probable Cause

Hill next argues that the Peña Affidavit failed to set forth probable cause that the HILL Email Account would contain evidence of the crimes listed in the affidavit, including 18 U.S.C. §§ 1956 and 1957 (money laundering and money laundering conspiracy); 18 U.S.C. § 1960 (operating an unlicensed money transmitting business); 50 U.S.C. §§ 1705, Executive Orders 13660, 13661, and 13662, and 31 C.F.R. § 589.201 (violations of the International Emergency Economic Powers Act and evading sanctions imposed by OFAC); and 31 U.S.C. §§ 5318 and 5322 (Bank Secrecy Act violations) (the “Subject Offenses”). But this argument fares no better than the last. As further discussed below, there was ample probable cause to believe that evidence of the Subject Offenses, including evidence confirming HILL’s own connection to Samurai and participation in the Subject Offenses, would be found in the HILL Email Account.

1. Applicable Law

“The law is well established that probable cause to search a location for . . . particular items or records is demonstrated where a totality of circumstances indicates a ‘fair probability that contraband or evidence of a crime will be found’ thereby.” *Lauria*, 70 F.4th at 128 (quoting *Gates*, 462 U.S. at 238). The standard does not demand “hard certainties,” *Gates*, 462 U.S. at 231, but rather is “grounded in sufficient facts to establish the sort of ‘fair probability’ on which ‘reasonable and prudent men, not legal technicians’ act.” *Lauria*, 70 F.4th at 128 (quoting *Gates*, 462 U.S. at 231); see *Florida v. Harris*, 568 U.S. 237, 244 (2013) (describing probable cause as “practical,” “common-sensical,” “all-things-considered” standard for assessing probabilities in particular factual context); *United States v. Esters*, No. 21 Cr. 398 (EK), 2022 WL 16715891, at *4 (E.D.N.Y. Nov. 4, 2022) (“Generally speaking, probable cause is a low bar, requiring only a ‘fair probability’ that a crime has been or is being committed; it does not mean more likely than not.”). Demonstrating a nexus between the criminal activities alleged and the place or object to be searched “does not require direct evidence and may be based on reasonable inference from the facts presented based on common sense and experience.” *United States v. Welch*, No. 24 Cr. 79 (ALC), 2025 WL 1380063, at *3 (S.D.N.Y. May 13, 2025) (quoting *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004)). Additionally, the Second Circuit has “recognized that a law enforcement officer’s experience and training may permit the officer to discern probable cause from facts and circumstances where a layman might not.” *United States v. Babilonia*, 854 F.3d 163, 178 (2d Cir. 2017).

2. Discussion

Hill attempts to suggest that the Peña Affidavit lacked probable cause that there would be evidence of violations of 18 U.S.C. § 1960 in the HILL Email Account because the Peña Affidavit

conceded that Samourai advertised itself as a “non-custodial wallet, meaning that Samourai users do not share with Samourai the ‘private keys’ that owners of cryptocurrency use to control their cryptocurrency holdings.” (Peña Affidavit ¶ 9(a)). But this argument fails for the same reasons described above that Rodriguez and Hill’s motion to dismiss the 18 U.S.C. § 1960 count in the Indictment fails. *See supra* at 26-29. Namely, the evidence shows that Samourai in fact operated as a money transmitter for purposes of 18 U.S.C. § 1960, even if individual users maintained exclusive control over their private keys. In any event, even if the Court were to find that Samourai could not qualify as a matter of law as a money transmitting business for purposes of 18 U.S.C. § 1960, there was still probable cause that the defendants still conspired to operate Samourai to launder money and to evade sanctions, and the Peña Affidavit contained ample probable cause that evidence of those crimes would be found in the HILL Email Account.

Relating to Samourai as a whole, the Peña Affidavit presented evidence that, among other things:

- Samourai was a cryptocurrency business that offered multiple services to customers that could be used by criminals to launder proceeds of criminals on the Internet, including a mixing service called “Whirlpool” and a transmission service named “Ricochet” that allowed a user to build in four intermediate transactions whenever a user was sending cryptocurrency to another wallet (Peña Affidavit ¶ 8);
- Samourai collected a fee for all these transactions but was not registered as a money transmitting business (Peña Affidavit ¶ 8);
- Law enforcement reports identified over \$700 million in cryptocurrency that had been received into wallets provided by Samourai between in or around 2015 and the present (Peña Affidavit ¶ 9(d));
- Over \$150 million in cryptocurrency that is linked to known dark web marketplaces, sanctioned wallets/entities, and scams have been deposited into wallets that are known to be provided by Samourai (Peña Affidavit ¶ 9(d));
- Samourai’s messages on Twitter showed that the operators of Samourai encouraged users to download the wallet so they could engage in anonymous financial transactions

without concern for collection of know-your-customer information frequently collected by financial institutions and cryptocurrency exchanges (Peña Affidavit ¶¶ 17(a); 18(a));

- Samourai’s operators encouraged sanctioned Russian entities on Twitter to evade sanctions by engaging in cryptocurrency transactions on Samourai Wallet (Peña Affidavit ¶ 17(b));
- Samourai’s operators encouraged “refugees” from other cryptocurrency mixers that were planning to be more cooperative with law enforcement on Twitter (Peña Affidavit ¶¶ 17(c); 18(b));
- Samourai’s operators also posted messages in a Telegram account responding to questions about how to use Samourai, including how to avoid getting caught when adding cryptocurrency from a cryptocurrency exchange and a darknet market simultaneously (Peña Affidavit ¶ 21(b)); and
- A search of two Samourai-related email addresses revealed a PowerPoint slide deck from 2015 noting that Samourai’s customers would include “Dark/Grey Market participants.” (Peña Affidavit ¶ 22(a)).

Putting all these facts together, the Peña Affidavit showed that Samourai was operating as a money laundering service for customers and actively encouraging criminals to use their service to engage in sanctions evasion and launder criminal proceeds. The Peña Affidavit also explained that Samourai had multiple features, including Whirlpool and Ricochet, designed to conceal the proceeds of criminal activities from others, and a 2015 PowerPoint slide deck strongly suggested that Samourai from its inception was aware that its customer base would include criminal actors.

Next, the Peña Affidavit presented evidence explaining why evidence of Samourai’s operations, as well as Hill’s connection to Samourai, would likely be found in the HILL Email Account. The Peña Affidavit pointed out that the HILL Email Account had approximately 90 emails in its inbox from Samourai-related email accounts, including where Samourai was in the domain or usernames. (Peña Affidavit ¶ 23(b)). The Peña Affidavit laid out some of the email addresses that had been exchanging emails with the HILL Email Account, many of them containing Samourai-related domain names like samourai.io or samouriwallet.com, and other

email accounts connected to digital currency or business support email accounts, all highly suggesting that the HILL Email Account would contain evidence of Samourai-related communications, or other evidence of Samourai's day-to-day operations. (*Id.*). Finally, the Peña Affidavit contained information about Special Agent Peña's knowledge and experience with individuals engaging in fraudulent activities, including sanctions evasion, unlicensed money transmission, and laundering, and how those individuals stored evidence and records of their crimes in email accounts like the Subject Accounts. (Peña Affidavit ¶ 26). Putting together all of this evidence, Judge Gorenstein had an ample record for finding a "fair probability" that the HILL Email Account would contain evidence of the Subject Offenses, including evidence showing Hill's participation in Samourai, his communications with other Samourai employees or associates, as well as records, web searches, assets, transactional information, or other information that could assist in revealing the identities of the participants in Samourai. *Gates*, 462 U.S. at 238.

C. Magistrate Judge Gorenstein's Warrant Was Sufficiently Particularized and Not Impermissibly Overbroad

Hill also challenges the search warrant itself, arguing that the warrant lacked a specific search protocol, failed to provide meaningful guidance as to what types of evidence could be identified during the search of the email account, and was overbroad. But these arguments also fail. As set forth below, courts have declined to impose or require any specific search protocol in a search warrant. Moreover, the search warrant issued by Judge Gorenstein was sufficiently particularized to permit the executing officers to exercise rational judgment in determining what to seize, and the warrant's list of permissible items for seizure was sufficiently tailored to the

probable cause showing in the underlying affidavit. Accordingly, the Court should reject Hill's motion to suppress on these grounds.

1. Applicable Law

a. Manner of Search

“[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.” *Dalia v. United States*, 441 U.S. 238, 257 (1979). For searches authorizing the seizure of electronically stored information, “the Fourth Amendment does not require a search warrant to specify computer search methodology.” *United States v. Bowen*, 689 F. Supp. 2d 675, 681 (S.D.N.Y. 2010). Accordingly, courts “reviewing challenges to searches of electronically stored information have declined to require any particular protocols such as the use of specific search terms or methodologies.” *United States v. Lebovits*, No. 11 Cr. 134 (SJ), 2012 WL 10181099, at *22 (E.D.N.Y. Nov. 30, 2012). “The reason for not imposing such a requirement on law enforcement in conjunction with search warrant applications for computer searches is obvious—in most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities.” *Ray*, 541 F. Supp. 3d 355, 393 (S.D.N.Y. 2012) (quoting *United States v. Graziano*, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008)); *see also Ulbricht*, 858 F.3d at 102 (“[I]t will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search.”). “It has long been

perfectly appropriate to search the entirety of a premises or object as to which a warrant has issued based on probable cause, for specific evidence as enumerated in the warrant, which is then to be seized.” *United States v. Barrett*, No. 23 Cr. 623 (JLR), 2025 WL 371084, at *22 (S.D.N.Y. Feb. 3, 2025) (quoting *United States v. Ulbricht*, No. 14 Cr. 68 (KBF), 2014 WL 5090039, at *14 (S.D.N.Y. Oct. 10, 2014)). “[T]raditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are.” *Ulbricht*, 858 F.3d at 100.

b. Particularity

To satisfy the Fourth Amendment’s particularity requirement, a warrant must: (1) “identify the specific offense for which the police have established probable cause”; (2) “describe the place to be searched”; and (3) “specify the items to be seized by their relation to designated crimes.” *United States v. Purcell*, 967 F.3d 159, 178 (2d Cir. 2020) (internal quotations omitted). “The Fourth Amendment does not require a perfect description of the data to be searched and seized, however,” and “[s]earch warrants covering digital data may contain ‘some ambiguity. . . .’” *United States v. Ulbricht*, 858 F.3d 71, 100 (2d Cir. 2017) (quoting *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013)) . Because a warrant’s description of items to be seized need only be “sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize,” a warrant is sufficiently particular when it limits the scope of the search to evidence of particular federal crimes and gives an “illustrative list of seizable items.” *United States v. Folks*, No. 20-3267-cr, 2021 WL 5987009, at *1 (2d Cir. Dec. 17, 2021); *see also Riley*, 906 F.2d at 843-845 (similar); *United States v. Wallace*, No. 24 Cr. 411 (MKV), 2025 WL 1435066, at *5 (S.D.N.Y. May 19, 2025) (collecting cases holding that particularity requirement

is satisfied where search warrant authorized review of ESI that “amounts to evidence, fruits, and or instrumentalities of the Subject Offenses and also provided twelve sub-categories with respect to what the evidence, fruits, and instrumentalities might be”).

c. Overbreadth

“The doctrine of overbreadth represents, in a sense, an intersection point for probable cause and particularity principles: it recognizes, in pertinent part, that a warrant’s unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause.” *United States v. Wey*, 256 F. Supp. 3d 355, 382 (S.D.N.Y. 2017). The overbreadth doctrine thus requires that the warrant’s description of the objects to be seized not be “broader than can be justified by the probable cause upon which the warrant is based.” *Galpin*, 720 F.3d at 446. “[A] warrant is legally invalid for overbreadth to the extent it permits officers to search or seize items without probable cause that they contain evidence of a crime.” *United States v. Kidd*, 386 F. Supp. 3d 364, 374 (S.D.N.Y. 2019). “[B]readth and particularity are related but distinct concepts.” *Ulbricht*, 858 F.3d at 102. “A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement.” *Id.* Broad language in a search warrant may be justified if the criminal methods are extensive and the criminal activity is pervasive. For example, “[w]hen the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements.” *Id.* (quoting *U.S. Postal Serv. v. C.E.C. Servs.*, 869 F.2d 184, 187 (2d Cir. 1989)).

2. Discussion

Applying the principles set forth above, Hill's attacks on the email search warrant are without merit. To begin with, Hill argues that it was impermissible for Magistrate Judge Gorenstein to issue a warrant that authorized law enforcement agents to conduct a file-by-file review of the HILL Email Account to search for evidence, rather than requiring law enforcement agents to use targeted search tactics or other substantive limitations on the types of files they would have been permitted to search. But courts have consistently declined to impose those types of limitations on searches of electronic data. *See, e.g., Ray*, 541 F. Supp. 3d 355, 393 (S.D.N.Y. 2021) ("[R]ay's argument that the warrant should have required the agents to use specific search terms or keywords in their search finds no support in the law of this Circuit." (collecting cases)). The Second Circuit "has analogized searches of entire electronic devices to warrants 'allow[ing] the government to search a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence.'" *United States v. Arias Casilla*, No. 21 Cr. 218-1 (AT), 2022 WL 2467781, at *6 (S.D.N.Y. July 6, 2022) (quoting *Ulbricht*, 858 F.3d at 102-03); *see also United States v. Gatto*, 313 F. Supp. 3d 551, 560 (S.D.N.Y. 2018) (explaining that warrants are not rendered invalid "by virtue of their having authorized searches of the entirety of the cell phones for data responsive to the warrants"). Similarly, Hill cannot claim that it was unlawful for Magistrate Judge Gorenstein to issue a search warrant allowing law enforcement officers to conduct a file-by-file review of the HILL Email Account for evidence of the Subject Offenses, merely because the HILL Email Account was also a personal email account that Hill used for non-criminal purposes. *See Ray*, 541 F. Supp. 3d at 394 ("The Fourth Amendment does not prohibit law enforcement from seizing, pursuant to a warrant, electronic devices that are likely to contain evidence of crime simply because that

evidence is likely intermingled with other non-criminal and private information.”); *United States v. Rosario*, No. 19 Cr. 807 (LAP), 2021 WL 5647879, at *7 (S.D.N.Y. Dec. 1, 2021) (explaining that “the Court of Appeals has not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants”).

Hill next argues that some of the categories of information that the search warrant identified as evidence, fruits, and instrumentalities of the Subject Offenses lacked sufficient particularity, including: (1) “information identifying the user(s) of the Subject Accounts and the individuals involved in the Subject Offenses as well as their location(s)”; (2) “[e]vidence that may reveal the identifies of and/or relationships between Samourai’s creators, operators, management, and associates”; and (3) “[e]vidence that may identify assets, including bank accounts and digital or virtual currency accounts, that may represent proceeds of the Subject Offenses.” But none of these categories of evidence was so vague that it turned the search warrant for the HILL Email Account into a general warrant with no guidance to law enforcement whatsoever. For example, “user attribution evidence is analogous to the search for indicia of occupancy while executing a search warrant at a residence and can enable the Government to both prove the relevant crime and exclude the innocent from further suspicion.” *United States v. Motovich*, No. 21 Cr. 497 (WFK), 2024 WL 2943960, at *13 (E.D.N.Y. June 11, 2024). Similarly, the other categories disputed by Hill either contain explicit references to “Samourai”—the name of the criminal enterprise under investigation, or references to the Subject Offenses themselves, which is all that courts have required to satisfy particularity. *See Folks*, 2021 WL 5987009, at *1. Ultimately, this Court should find—as numerous other courts have found in materially similar circumstances—that the search warrant was “sufficiently particular to enable the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize.” *United*

States v. Aminov, No. 23 Cr. 110 (MKV), 2024 WL 3104526, at *4 (S.D.N.Y. June 24, 2024) (quoting *United States v. McDarragh*, 351 F. App'x 558, 561 (2d Cir. 2009) (summary order)). While the search warrant concededly “may contain some ambiguity . . . law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have [e]nsured that all those facts were included in the warrant.” *Id.* (quoting *Galpin*, 720 F.3d at 446)); *see also Riley*, 906 F.2d 841, 844-45 (2d Cir. 1990) (“[A]llowing some latitude [regarding the warrant’s description of the category of items to be seized] simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked ‘drug records.’”).

Finally, Hill himself has not pointed to any materials that were marked as identified by law enforcement officers as being unjustifiably beyond the scope of the categories of evidence that were included in the search warrant. As Hill acknowledges, the Government ultimately marked approximately five documents in the HILL Email Account as identified data under the search warrant (*i.e.*, data that law enforcement could permissibly seize under the terms of the warrant), including: portions of the browser search history where Hill conducted searches for darknet marketplaces like “Silk Road,” the “Dread” darknet marketplace forum (where Hill advertised Samourai to darknet marketplace users), and the name of a Samourai investor (Mazur Decl. Exhs. 16 and 20); searches for airline flights circumstantially showing Hill’s location (Mazur Decl. Exhs. 17 and 18); and subscriber information showing that the HILL Email Account was linked to the dev@samouraiwallet.com account, was set for the Lisbon, Portugal timezone, and had numerous hardware and software features consistent with the user of the HILL Email Account being a software developer for Google Play Store applications like Samourai (Mazur Decl. Exh. 20). Given that law enforcement officers did not seize any improper evidence, but rather located and

seized highly probative evidence of the Subject Offenses during its search, the Court should not find that the search authorized by Magistrate Judge Gorenstein was insufficiently particularized or overbroad. *See Ray*, 541 F. Supp. 3d at 396 (denying motion to suppress search warrant as overbroad when “the defense has offered the Court no reason to doubt that the officers faithfully executed the warrant” (quoting *Ulbricht*, 858 F.3d at 103)).

D. The Good Faith Exception Clearly Applies Here

To the extent that Hill has identified any flaws in the search warrant—he has not—law enforcement agents were entitled to reasonably rely on the search warrant in good faith in conducting its search of the HILL Email Account.

1. Applicable Law

Under the “good faith” exception to the exclusionary rule, that rule and its remedy of suppression do not apply where evidence is “obtained in objectively reasonable reliance on a subsequently invalidated search warrant.” *United States v. Leon*, 468 U.S. 897, 922 (1984). In announcing this principle, the Supreme Court noted that suppression could have no deterrent impact on law enforcement agents who acted on the objectively reasonable assumption that their conduct did not violate the Fourth Amendment. *See id.* at 918-20. In analyzing the applicability of the good faith exception, the pivotal question is “whether a reasonably well trained officer would have known that the search was illegal despite the magistrate’s authorization.” *Id.* at 922 n.23. If the reviewing court finds that the officers’ reliance on the warrant was objectively reasonable, suppression is not warranted. *See, e.g., United States v. Singh*, 390 F.3d 168, 183 (2d Cir. 2004). Moreover, “[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Herring v. United States*, 555 U.S. 135, 144 (2009). Exclusion

should be a “last resort” rather than a “first impulse.” *United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010). The exclusionary rule should be used only where law enforcement “exhibit[s] deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights.” *United States v. Raymonda*, 780 F.3d 105, 117-18 (2d Cir. 2015) (quoting *United States v. Stokes*, 733 F.3d 438, 443 (2d Cir. 2013)).

As a result, “[s]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.” *Leon*, 468 U.S. at 922; *see also Golino v. City of New Haven*, 950 F.2d 864, 870 (2d Cir. 1991) (noting that “issuance of a warrant by a neutral magistrate, which depends on a finding of probable cause, creates a presumption that it was objectively reasonable for the officers to believe that there was probable cause”). Indeed, the good faith exception is inapplicable only in four narrow circumstances:

- (1) Where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992).

2. Discussion

Hill argues that the search warrant in this case was facially deficient and could not be reasonably relied upon based on the breadth of the categories of evidence to be seized in the search warrant, law enforcement’s review of the entirety of the HILL Email Account, and the fact that law enforcement had already seized and located some evidence of Hill’s participation in Samourai through other sources. But none of these arguments suggests that law enforcement here was acting in bad faith when they executed Judge Gorenstein’s search warrant.

As described above, courts have regularly approved search warrants containing permission for law enforcement to seize evidence of “user attribution” so that criminals cannot argue at trial that someone else was using their email account to commit the Subject Offenses. As Special Agent Peña noted in her affidavit, “user attribution” evidence is analogous to “indicia of occupancy” while executing a search warrant at a residence and is important for showing who was using or in control of an email account at a particular time. (Peña Affidavit at 4(e)). Hill attempts to suggest that this case is like *Wey*, where the Court found that a warrant was deficient because it set forth “expansive categories of often generic items subject to seizure—several of a ‘catch-all’ variety—without, crucially, any linkage to the suspected criminal activity, or indeed any meaningful content-based parameter or other limiting principle.” 256 F. Supp. 3d at 385. But the search warrant here bears no resemblance whatsoever to the search warrant in *Wey*. Unlike in *Wey*, the search warrant in this case contained specific identifications of the relevant Subject Offenses, as well as a list of example materials to be seized as evidence of the Subject Offenses. *Cf. id.* at 387 (finding particularity requirement not met where warrant authorized seizure of sweeping categories of materials, regardless of their potential connection to any suspected criminal activities). The search warrant here is much more similar to the post-*Wey* line of cases, all finding that search warrants are sufficiently particularized when they clearly described a set of specified federal crimes and an illustrative list of items to be seized. *See Barrett*, 2025 WL 371084, at *19 (“The form that the search warrants in this case took is a typical one and one frequently upheld by the courts: that is, the warrants broadly describe[d] the items to be seized as evidence, fruits, or instrumentalities of specified federal crimes, and also set[] forth an illustrative list of items to be seized.”); *United States v. Jacobson*, 4 F. Supp. 3d 515, 524 (E.D.N.Y. 2014) (“The reference to particular offenses and the use of an illustrative list of items to seize sufficiently particularized the

warrants.”).

Similarly, the fact that law enforcement had already collected some evidence that Hill was involved in Samourai through publicly available information and other searches of Samourai-related email accounts does not mean that law enforcement officers searched the HILL Email Account in bad faith. Hill has cited to no caselaw, and the Government is aware of none, suggesting that law enforcement officers are barred from seeking search warrants for additional evidence of facts that it may already believe to be true. Given that the Government ultimately bears the burden of proving a defendant’s guilt beyond a reasonable doubt at trial, law enforcement officers acted entirely properly in seeking additional corroborating evidence from the HILL Email Account—an email account whose username is registered in his name—that Hill was in fact the user of the dev@samouraiwallet.com email account that had been serving as one of the key operators of Samourai. As described above, law enforcement officers had also identified a series of approximately 90 emails from header information from the HILL Email Account suggesting that the account had been used to send and receive Samourai-related emails. Combined with the other evidence of Hill’s participation in Samourai, law enforcement officers reasonably believed there was probable cause that evidence of Samourai and Hill’s participation in Samourai would be found inside of the HILL Email Account. Nothing more is required. Additionally, the case law is clear that the fact that Samourai-related emails would likely be intermingled with personal or private emails does not impact the appropriateness of seeking a search warrant in these circumstances. *See Ulbright*, 858 F.3d at 102 (explaining that a “warrant may allow the government to search a suspected drug dealer’s entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence”); *Ray*, 541 F. Supp. 3d at 394 (“The Fourth Amendment does not prohibit law enforcement from seizing,

pursuant to a warrant, electronic devices that are likely to contain evidence of crime simply because that evidence is likely intermingled with other non-criminal and private information.”). Based on this record, the Court should find that law enforcement agents were entitled to rely in good faith on the search warrant issued by Judge Gorenstein.

E. The Full Extraction of Hill’s Email Account Is Needed for Purposes of Authenticating Identified Data at Trial

Finally, Hill requests that the Court order the Government to return or delete the full contents of the HILL Email Account under Federal Rule of Criminal Procedure 41(g). But forcing the Government to purge any copies of the HILL Email Account at this stage of the proceedings would create challenges for authenticating identified data from the HILL Email Account at trial. At trial, the Government anticipates calling a custodian witness from Google to confirm that all of its proposed exhibits from the HILL Email Account are authentic copies of data that Google provided in its response to the search warrant. The primary way for a Google custodian to provide such authentication is to compare the hash value¹⁷ of the entire HILL Email Account in the possession of law enforcement with the hash value prepared by Google when the data was first provided to law enforcement. Additionally, to the extent that Hill may seek to provide emails from the HILL Email Account in his defense at trial, one of the only ways for the Government to similarly verify the authenticity of these emails is to request that a Google custodian compare the contents of the email with the version of the email that came from the original data provided by Google to law enforcement in response to the search warrant. As the Second Circuit recognized in *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016):

¹⁷ A hash value is a fixed-size string of characters generated by inputting a batch of original data into hash function. The hash value then acts as a unique identifier for original data, making it useful for verifying data integrity and authenticity.

[T]he Government plausibly argues that, because digital storage media constitute forensic objects with contours more complex than—and materially distinct from—file cabinets containing interspersed paper documents, a digital storage medium or its forensic copy may need to be retained, during the course of an investigation and prosecution, to permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant; to secure metadata and other probative evidence stored in the interstices of the storage medium; and to preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained.

Id. at 216; *see also Ramsden v. United States*, 2 F.3d 322, 326 (9th Cir. 1993) (“The United States’ retention of the property generally is reasonable if it has a need for the property in an investigation or prosecution.”). Other courts have similarly recognized that the Government should not be compelled to return electronic devices to defendants when it plans to introduce the electronic evidence at trial. *See United States v. Messalas*, 612 F. Supp. 3d 93, 112 (E.D.N.Y. 2020) (“The Government has more than adequately justified its retention of the iPhone on the basis that it plans to introduce the phone as evidence at trial and the data on the phone cannot be exactly copied.”); *United States v. Wilburn*, Nos. 19 Cr. 108 (EK) (VMS), 19 Cr. 139 (EK) (VMS), 2024 WL 1142297, at *4 (E.D.N.Y. Mar. 15, 2024) (explaining that Government could not feasibly separate “innocent digital data” from contraband). Based on this record, the defendant cannot show that the Government’s retention of the full extraction of the HILL Email account is unreasonable. *See Allen v. Grist Mill Capital LLC*, 88 F.4th 383, 396 (2d Cir. 2023) (holding that “the defendant bears the burden of demonstrating that the government’s retention of the seized property is unreasonable”).

III. Hill’s Motion to Sever Should Be Denied

Hill argues that he should be tried separately from Rodriguez, alleging that Rodriguez would be willing to provide exculpatory testimony for Hill at a separate trial in support of a potential good faith or advice-of-counsel defense. But Hill has completely failed to meet his burden of showing that Rodriguez will be willing to testify at a subsequent trial, or that Rodriguez’s

testimony is necessary to support his defense. Courts have routinely denied these kinds of unsubstantiated and speculative requests for severances based on potential co-defendant testimony, especially in cases like this one where separate trials would create a severe strain on judicial resources.

A. Applicable Law

As the Supreme Court has made clear, the interests of efficiency and consistency of outcome generally favor joint trials of defendants indicted together. *Zafiro v. United States*, 506 U.S. 534, 537-38 (1993) (explaining that joint trials promote efficiency and “serve the interests of justice by avoiding the scandal and inequity of inconsistent verdicts”); *see also United States v. Shareef*, 190 F.3d 71, 77 (2d Cir. 1999) (explaining in *Bruton* context that the burden of multiple trials in a single conspiracy requires that “prosecutors bring separate proceedings, presenting the same evidence again and again, requiring victims and witnesses to repeat the inconvenience (and sometimes trauma) of testifying, and randomly favoring the last-tried defendants who have the advantage of knowing the prosecution’s case beforehand.” (quoting *Richardson v. Marsh*, 481 U.S. 200, 210 (1987))). As a result, “a district court should grant a severance under Rule 14 only if there is a serious risk that a joint trial would compromise a specific trial right of one of the defendants, or prevent the jury from making a reliable judgment about guilt or innocence.” *Id.* at 539; *see also United States v. Barnes*, 979 F.3d 283, 316 (5th Cir. 2020) (“As the district court correctly noted, the rule, rather than the exception, is that persons indicted together should be tried together, especially in conspiracy cases.”). The “defendant seeking severance must show that the prejudice to him from joinder is sufficiently severe to outweigh the judicial economy that would be realized by avoiding multiple lengthy trials.” *United States v. Page*, 657 F.3d 126, 129 (2d Cir. 2020).

Defendants frequently request severances because they “might suffer prejudice if essential exculpatory evidence”—like a co-defendant’s potentially helpful testimony—would only be “available to a defendant tried alone.” *Zafiro*, 506 U.S. at 539. In determining whether to grant a severance on this basis, the Second Circuit has stated that the following factors should be considered: “(1) the sufficiency of the showing that the co-defendant would testify at a severed trial and waive his Fifth Amendment privilege; (2) the degree to which the exculpatory testimony would be cumulative; (3) the counter arguments of judicial economy; and (4) the likelihood that the testimony would be subject to substantial, damaging impeachment.” *United States v. Wilson*, 11 F.3d 346, 354 (2d Cir. 1993) (quoting *United States v. Finkelstein*, 526 F.2d 517, 523-24 (2d Cir. 1975)). Courts are not constrained to these factors; the factors “merely define the perimeters of the severance question—the crucial inquiry remains whether the [defendants] were so prejudiced by a joint trial under these circumstances that severance should have been granted.” *Finkelstein*, 526 F.2d at 523.

With respect to the first factor, the Second Circuit has repeatedly found that offers to testify by a co-defendant that are “expressly conditioned on [the defendant] being tried last”—just like Rodriguez’s conditional offer to testify here—is “a condition which smacks of bad faith.” *United States v. Bari*, 750 F.2d 1169, 1178 (2d Cir. 1984); *see also United States v. Spinelli*, 352 F.3d 48, 56 (2d Cir. 2003) (“Michael had offered to testify to Spinelli’s innocence, but only if Spinelli were tried separately and subsequently. We have, however, noted that such conditional offers smack of bad faith.”). Additionally, when the co-defendant witness has pleaded not guilty, it strongly indicates that the potential witness is “unlikely to waive the privilege against self-incrimination at a separate trial unless they had already been acquitted.” *Bari*, 750 F.2d at 1177; *see also United States v. O’Connor*, 650 F.3d 839, 861 (2d Cir. 2011) (“Sacco here chose to stand trial and not to

testify in his own behalf; O'Connor has proffered no reason to believe that he would waive his Fifth Amendment privilege in order to testify at a trial of O'Connor alone.”).

Similarly, courts have routinely denied severance requests where the allegedly exculpatory testimony by a co-defendant is cumulative because a defendant could testify to the same subject matter. *See Wilson*, 11 F.3d at 354 (finding no abuse of discretion where a trial court held that “testimony would be cumulative, given that [the defendant] could have called any number of witnesses, including himself”); *United States v. Levy*, No. 11 Cr. 62 (PAC), 2013 WL 787913, at *2 (S.D.N.Y. Mar. 4, 2013) (“[C]ourts have discounted this showing under the second *Finkelstein* factor when defendants could otherwise testify as to such facts.”); *United States v. Gershman*, No. 16 Cr. 553 (BMC), 2018 WL 3038498, at *1 (E.D.N.Y. June 19, 2018) (explaining that the allegedly exculpatory testimony is cumulative because “[f]or one thing, Gershman himself could testify as to the same subject matter”); *United States v. Schlegel*, No. 06 Cr. 0550 (JS), 2009 WL 3837305, at *2 (E.D.N.Y. Nov. 16, 2009) (“[T]he Court rejects Brooks’ claim that he cannot provide testimony on his own behalf regarding certain aspects of the accounting fraud allegations because Brooks was not personally involved in valuing the inventory. Clearly, Brooks can provide information regarding his alleged lack of involvement with the inventory valuation.”).

B. Discussion

Applying the principles set forth above, Hill’s request for a severance should be denied because he has failed to satisfy any of the relevant factors described above:

First, Hill has not shown that Rodriguez will waive his Fifth Amendment privilege and testify for Hill at a subsequent trial. As noted above, Rodriguez’s purported willingness to testify for Hill—only on the condition that Hill is tried second—“smacks of bad faith,” *Bari*, 750 F.2d at 1177, and numerous courts have given little weight to these types of conditional offers to testify.

Rodriguez’s conditional offer to testify is also premised on the notion that Rodriguez would no longer have any Fifth Amendment concerns if his trial proceeded first. But that is plainly wrong as a matter of law. *See Schlegel*, 2009 WL 3837305, at *2; *United States v. Triumph Capital Group*, 260 F. Supp. 2d 432, 443 (D. Conn. 2002) (explaining that Fifth Amendment concerns continue after a defendant’s trial, specifically if the defendant was “convicted in an earlier trial and had a motion or appeal pending that challenged his conviction and could result in a new trial”); *Gershman*, 2018 WL 3038498, at *1) (“It strains credulity to imagine that Tsvetkov would testify if he were convicted (with a pending appeal likely), or if he were acquitted (because doing so could expose him to other charges dropped from the last indictment).”); *see also Minnesota v. Murphy*, 465 U.S. 420, 426 (1984) (holding that a defendant’s Fifth Amendment privilege continues after he has been convicted). Even if Rodriguez had no pending appeal at the time of Hill’s trial, the Government would likely still cross-examine him about other potential Samurai-related crimes to which he could still be charged in the future, including, for example, substantive money laundering charges, substantive money transmission offenses, sanctions evasion, misprision of a felony, and tax evasion. For these reasons, Hill has failed to demonstrate that Rodriguez will be willing to testify at his trial. As the Second Circuit has clearly held, “[s]elf-serving, conclusory statements that exculpatory witnesses will not testify at a joint trial are not adequate to compel severance.” *Bari*, 750 F.2d at 1177. Hill’s motion for a severance should be denied on this basis alone.

Second, Hill has failed to show that Rodriguez’s testimony is necessary or helpful for his advice of counsel or good faith claims. At the outset, Hill provides no detail regarding the substance of Rodriguez’s allegedly exculpatory testimony, suggesting that Rodriguez will testify about “discussions with Mr. Hill concerning the legality of Samurai under United States law,

including discussions based on Mr. Rodriguez’s own communications with outside counsel.” (Docket No. 103 at 10). But Hill has not said anything about the substance of these discussions between Hill and Rodriguez, or between Rodriguez and outside counsel. Based on this sparse record, the Court and the Government have no meaningful ability to assess whether these alleged conversations are relevant or admissible. *See Bari*, 750 F.2d at 1177 (“The substance of the allegedly exculpatory testimony is not detailed in the various affidavits, and we are thus unable to weigh the importance of any of that testimony against the evidence presented against [the defendant] at trial.”); *United States v. Fox*, No. 22 Cr. 53 (JLS) (JJM), 2023 WL 6940197, at *5 (W.D.N.Y. Oct. 20, 2023) (“Further, the lack of specific detail regarding several aspects of Dellavalle’s purported testimony also weighs against severance.”).

The viability or relevance of any advice of counsel or good faith defense is especially remote in light of the Government’s decision to no longer proceed with charges relating to Samourai’s failure to register with FinCEN as an unlicensed money transmitter under 18 U.S.C. § 1960(b)(1)(B). Given that the focus of the trial will be on Hill and Rodriguez’s roles in large scale money laundering and transmission of criminal proceeds using Samourai, it is highly unlikely that any of these purported, unspecified conversations between Hill and Rodriguez will be relevant to the charges at trial. The Court should be skeptical that any lawyer would advise Rodriguez and Hill that they faced no risk of being criminally charged for actively encouraging and soliciting criminals like hackers, sanctions evaders, and darknet drug traffickers to use their cryptocurrency mixing service, especially after the arrests and prosecutions of numerous other similarly situated cryptocurrency mixers like Helix, Bitcoin Fog, Tornado Cash, and ChipMixer.

To the extent that Hill has any valid advice of counsel or good faith defense here—which Hill has failed to otherwise show in his motion—Hill also cannot show that Rodriguez’s testimony

would not be cumulative of Hill’s own testimony about his conversations with Rodriguez, his contemporaneous notes of conversations with Rodriguez, and the attorney’s own testimony about what he or she told Rodriguez. Combined with the Government’s strong evidence that Hill and Rodriguez were the primary owners and operators of Samurai and were partners in the Samurai criminal conspiracy, the jury will have no reason to believe that Rodriguez would have failed to pass along any helpful legal advice received from outside counsel to give Hill comfort that he was not violating the law. Given Hill’s own ability to testify about his state of mind, any testimony by Rodriguez would be cumulative. *See Gershman*, 2018 WL 3038498, at *1) (finding co-defendant testimony to be cumulative because the defendant could testify as to the same subject matter (collecting cases)); *see also Wilson*, 11 F.3d at 354 (finding no abuse of discretion where a trial court held that “testimony would be cumulative, given that [the defendant] could have called any number of witnesses, including himself”).

Additionally, the Government and the Court cannot even remotely assess the extent to which Rodriguez’s testimony would be subject to damaging impeachment, given Hill’s failure to provide an affidavit summarizing Rodriguez’s proposed testimony as part of his motion. Nonetheless, there are various reasons why Rodriguez’s testimony would be subject to potential impeachment. Courts have recognized that “a co-defendant indicted as part of the same alleged conspiracy is ‘likely to be subject to substantial, damaging impeachment if he testifies’ on behalf of the defendant.” *United States v. Bongiovanni*, Nos. 19 Cr. 227 (JLS) (MJR), 23 Cr. 37 (JLS) (MJR), 2023 WL 3143894, at *8 (W.D.N.Y. Apr. 28, 2023) (quoting *United States v. Levy*, 2013 WL 787913, at *2); *Schlegel*, 2009 WL 3837305, at *3 (noting that co-defendant’s “testimony would be subject to impeachment” because she and the defendant allegedly “jointly participated in the alleged conspiracies for which they [were] charged”). Rodriguez would be especially

subject to damaging impeachment at Hill’s trial because of the escape plan that law enforcement discovered in Rodriguez’s home on the date of his arrest. As the Court will recall from the bail hearings in this matter, the escape plan found in Rodriguez’s home clearly contemplated that Rodriguez and Hill would flee from their respective locations and meet in Cyprus in the event that they became fugitives because of a law enforcement takedown of Samourai. *See* Docket No. 55 at 4-6; (Ind. ¶ 35). The escape plan—combined with all the other evidence of Rodriguez and Hill’s close and tight-knit relationship—would raise significant questions about Rodriguez’s credibility, particularly with respect to any argument that Rodriguez and Hill were both acting in good faith and believed that they were not at risk of being arrested for their conduct. (*See also* Ind. ¶¶ 24 (Rodriguez private Telegram message that poor mixing “is likely to get someone locked up”); 25.d (Hill tweet that poor mixing will lead to “inevitable arrests”); 26 (Rodriguez tweet expressing his knowledge of and lack of respect for federal criminal money laundering laws); 41 (Rodriguez tweet that “We rather sit in a jail cell than comply with KYC/AML requirements for Bitcoin.”)).

In support of his severance motion, Hill points to only one case from within the Second Circuit from over 45 years ago where a district court granted a defendant’s motion for severance so that a co-defendant could provide potentially exculpatory testimony. *See United States v. DePalma*, 466 F. Supp. 920, 921-23 (S.D.N.Y. 1979). But *DePalma* bears no resemblance to the facts of this case and only highlights how the defendant has failed to satisfy his burden here for a severance. In *DePalma*, the proposed co-defendant witness submitted an affidavit stating that he would waive his Fifth Amendment privilege and testify at a separate trial and setting forth the substance of the proposed testimony. *Id.* at 922. Additionally, before the motion was granted, the co-defendant witness took the stand in a *voir dire* before the Court and was cross-examined by

the Government. *Id.* The Court was able to make a finding that the proposed testimony would not be subject to substantial impeachment or otherwise cumulative with other evidence in the case. *Id.* at 922-23. In this case, the Court is unable to make any of those findings because Hill has provided virtually no information in support of his motion, and there are significant doubts about whether Rodriguez's testimony will be available, necessary, or helpful to Hill's defense.

Finally, the Government underscores that the trial in this case will be lengthy, costly, and very inconvenient for civilian witnesses, victims, expert witnesses, and potential jurors. Because Samourai's money laundering scheme was sprawling and involved the proceeds of many specified unlawful activities, the Government currently anticipates that trial in this matter will take approximately three to four weeks and will include multiple expert witnesses testifying at significant expense to the Government, victims and civilian witnesses who will be testifying about crimes that generated the criminal proceeds, and law enforcement witnesses from all around the country who will be traveling to New York City to testify. Additionally, the Government anticipates an overwhelming overlap in the presentation of evidence between a joint trial versus separate trials because the charges and key evidence are identical for each defendant. Given how costly and wasteful it would be to do a substantially similar trial twice in this case, the Government respectfully submits that the defendant has fallen far short of demonstrating that a joint trial here would compromise his rights or otherwise prevent the jury from making a reliable judgment about his guilt.

IV. The Defendants' Demand for Additional Disclosure and a Hearing Should Be Denied

The defendants ask the Court to (1) compel additional disclosures in connection with an August 23, 2023 phone call between members of the prosecution team and employees of the U.S.

Financial Crimes Enforcement Network (“FinCEN”);¹⁸ and (2) hold a hearing to inquire into the timing of the disclosure of the August 23, 2023 phone call, which defendants deem “a late disclosure of *Brady* information.” The parties have previously addressed the disclosure at length. (Dkts. 86 (Defendants’ letter motion), 88 (Government’s opposition), 89 (Defendants’ reply)). For all the reasons stated in the Government’s prior opposition—namely that there has been no *Brady* violation because the information disclosed in good faith is not *Brady* material and because the defendants have received the information with ample time before pretrial motions and trial—the Court should deny the defendants’ requests.

Moreover, since the parties last briefed the Court regarding the disclosure of the August 23, 2023 call with employees of FinCEN, the disclosed information has become wholly irrelevant to the charged conduct to be proven at trial. In response to a memorandum dated April 7, 2025, “Ending Regulation by Prosecution,” by the Deputy Attorney General, the Government is not

¹⁸ On May 2, 2025, in response to the defendants’ April 30, 2025 request for supplemental disclosure regarding the August 23, 2023 call, the Government produced “in an abundance of caution and in good faith,” among other things, (1) all substantive email correspondence between the prosecution team and members of FinCEN relating to the August 23, 2023 call, which consisted of a single email chain sent in preparation for the call, and (2) an email summary of the August 23, 2023 call, prepared by a member of the prosecution team and sent to unit supervisors immediately after the call. In the email correspondence with members of FinCEN, one of the FinCEN employees referenced an “initial discussion back in May.” Defendants move to compel additional information regarding that May call. However, the Government informed defense counsel in its May 2, 2025 letter that “[t]he referenced discussion with FinCEN in May did not relate to Samourai Wallet and there are no further substantive communications with FinCEN regarding Samourai Wallet.” The Government does not know why the FinCEN employee referred to the separate May conversation as an “initial discussion.” In addition, defendants move to compel disclosure of redacted information in the email summary sent to unit supervisors. As the Government informed defense counsel in its May 2, 2025 letter, the redacted communications were either privileged or not responsive to the defendants’ requests. The defendants have articulated no basis to compel additional disclosures in the face of the Government’s good-faith disclosures. Compelling any further disclosures would be a purposeless fishing expedition.

proceeding to trial regarding any violations of Title 18, United States Code, Section 1960(b)(1)(B), which criminalizes the failure to comply with the money transmitting business registration requirements under Title 31, United States code, Section 5330, which registration requirements are administered by FinCEN. The Government has obtained a superseding indictment that both eliminates Section 1960(b)(1)(B) as a charge and any reference to Title 31 in the money laundering conspiracy charge. For the reasons described above in Section I.B., FinCEN has no authority or role in interpreting or administering Sections 1960(b)(1)(C) or 1956, the remaining charged conduct. The charged conduct to be proven at trial therefore in no way implicates or relates to FinCEN regulations and guidance, making any further inquiry into the August 23, 2023 call between the prosecution team and employees of FinCEN of no relevance.¹⁹

¹⁹ Judge Failla recently determined in a similar prosecution, in *United States v. Roman Storm*, No. 23 Cr. 430 (KPF), that this same disclosure was not *Brady* material and was irrelevant. A transcript of that court conference is attached hereto as Exhibit A. In that case, the defendant, who operated a noncustodial cryptocurrency mixing service like the defendants here (although using different technology), has been charged with conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business, and conspiracy to violate IEEPA. In that case, as well, for the same reason, the Government has abandoned prosecution under Section 1960(b)(1)(B). The defendant claimed the Government committed a *Brady* violation by failing to disclose in that case the August 23, 2023 call at issue in this case because the two cases share a supervisor and the call related to whether a cryptocurrency mixing service that did not take custody of its users' cryptocurrency would be required to register with FinCEN. Judge Failla rejected the allegation that there was a *Brady* violation and determined the information was irrelevant, stating "I don't think the views of FinCEN employees—even senior FinCEN employees that don't make its way into FinCEN policy—matter." *Storm*, No. 23 Cr. 430 (KPF), (May 30, 2025 Tr. ("Ex. A") at 19:8-10). This is especially true where the charges no longer involved Section 5330 of Title 31. (*Id.* at 14 (disclosure was no longer relevant to the remaining charges, which now only covered subsection (b)(1)(B) of Section 1960, because there was no overlap between Section 1960 and Section 5330)). Likewise, the private opinions of FinCEN employees do not matter here.

CONCLUSION

For the reasons set forth above, the defendants' motions should be denied.

Respectfully submitted,

NICOLAS ROOS
Acting Deputy United States Attorney,
Attorney for the United States,
Acting under Authority Conferred by
28 U.S.C. § 515

By: /s/

Andrew K. Chan
David R. Felton
Cecilia E. Vogel
Assistant United States Attorneys
(212) 637-1072 / 2299 / 1084

Dated: June 26, 2025
New York, New York